CLIを使用したNFSの管理

ONTAP 9

NetApp
May 09, 2024

目次

CLIを使用したNFSの管理 1
NFS のリファレンスの概要 1
NAS ファイルアクセスを理解する 1
NAS ネームスペース内でデータボリュームを作成および管理します 9
セキュリティ形式を設定する 15
NFSを使用したファイルアクセスの設定 20
NFSを使用したファイルアクセスの管理 58
サポート対象のNFSバージョンとクライアント 112
NFS と SMB のファイルとディレクトリの命名規則 116

CLIを使用したNFSの管理

NFS のリファレンスの概要

ONTAP には、 NFS プロトコルで使用できるファイルアクセス機能が含まれています。NFS サーバおよびエクスポートボリュームまたは qtree を有効にすることができます。

これらの手順は、次の状況で実行します。

- ONTAP NFSプロトコルの機能の範囲について理解する必要がある。
- NFSの基本的な設定ではなく、あまり一般的でない設定タスクとメンテナンスタスクを実行する。
- System Manager や自動スクリプトツールではなく、コマンドラインインターフェイス（ CLI ）を使用する必要がある。

NAS ファイルアクセスを理解する

ネームスペースとジャンクションポイント

ネームスペースとジャンクションポイントの概要

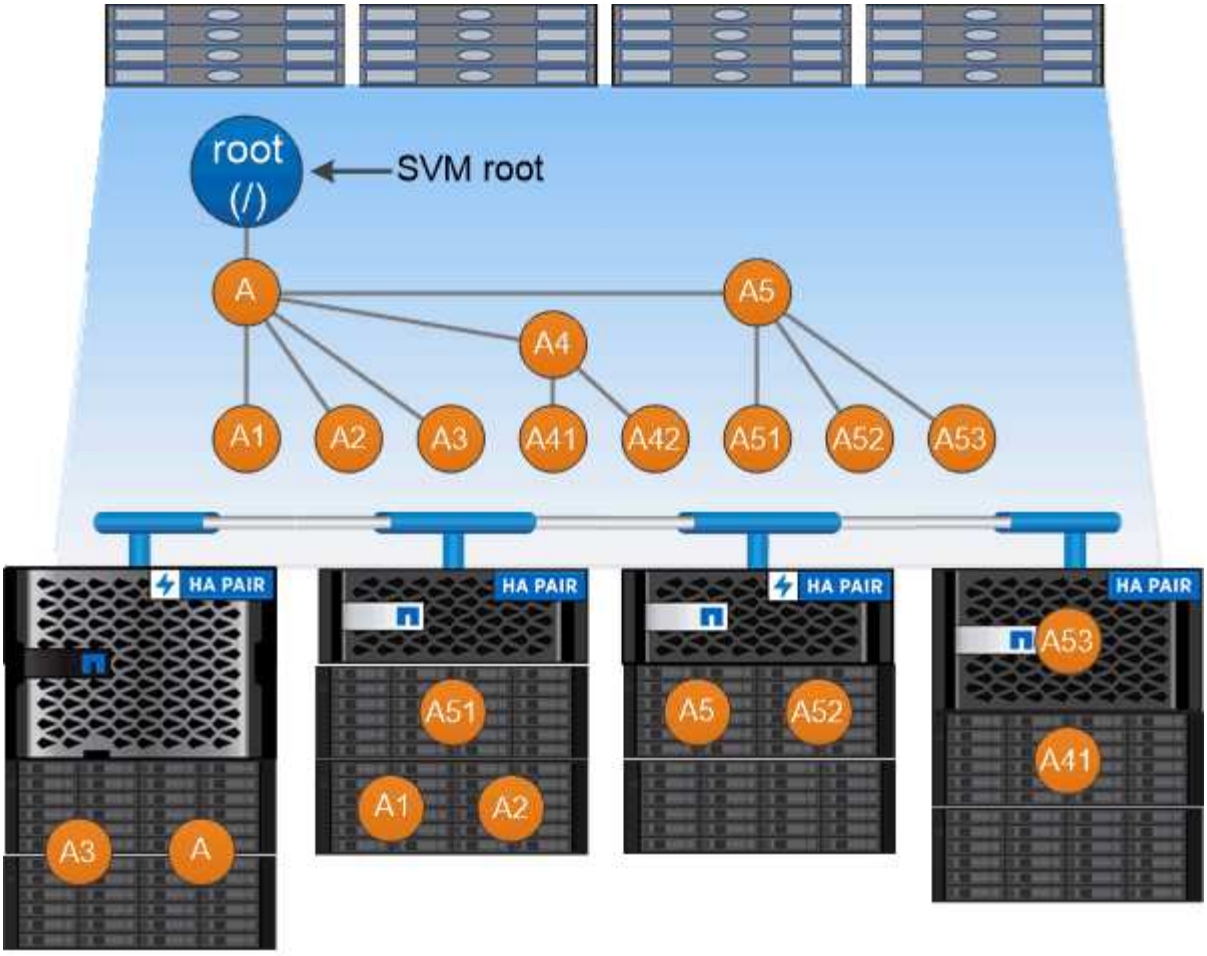
nas_namespace _ は、 _junction points_to によって結合されたボリュームを論理的にグループ化して、単一のファイルシステム階層を作成します。十分な権限を持つクライアントは、ストレージ内のファイルの場所を指定せずにネームスペース内のファイルにアクセスできます。ジャンクションされたボリュームはクラスタ内の任意の場所に配置できます。

NAS クライアントは、目的のファイルを含むすべてのボリュームをマウントするのではなく、 nfs_export_をマウントするか、 SMB_share にアクセスします。 _ エクスポートまたは共有は、ネームスペース全体またはネームスペース内の中間的な場所を表します。クライアントは、アクセスポイントより下にマウントされたボリュームにのみアクセスします。

ネームスペースには必要に応じてボリュームを追加できます。ジャンクションポイントは、親ボリュームジャンクションのすぐ下に作成することも、ボリューム内のディレクトリに作成することもできます。「vol3」という名前のボリュームのボリュームジャンクションへのパスは、になることがあります `/vol1/vol2/vol3`` または `/vol1/dir2/vol3`あるいは `/dir1/dir2/vol3`。このパスのことを _junction パスと呼びます。 _

SVM には、それぞれ一意のネームスペースがあります。SVM ルートボリュームは、ネームスペース階層へのエントリポイントです。

> ノードに障害やフェイルオーバーが発生したときにデータを引き続き利用できるようにするには、 SVM ルートボリュームに _load-sharing mirror_copy を作成する必要があります。



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

例

次の例は、ジャンクションパスがである「home4」という名前のボリュームをSVM vs1上に作成します `/eng/home`：

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

一般的な **NAS** ネームスペースアーキテクチャとは

SVM ネームスペースを作成するときに使用できる一般的な NAS ネームスペースアーキテクチャがいくつかあります。ビジネスやワークフローのニーズに合わせて、ネームスペースアーキテクチャを選択できます。

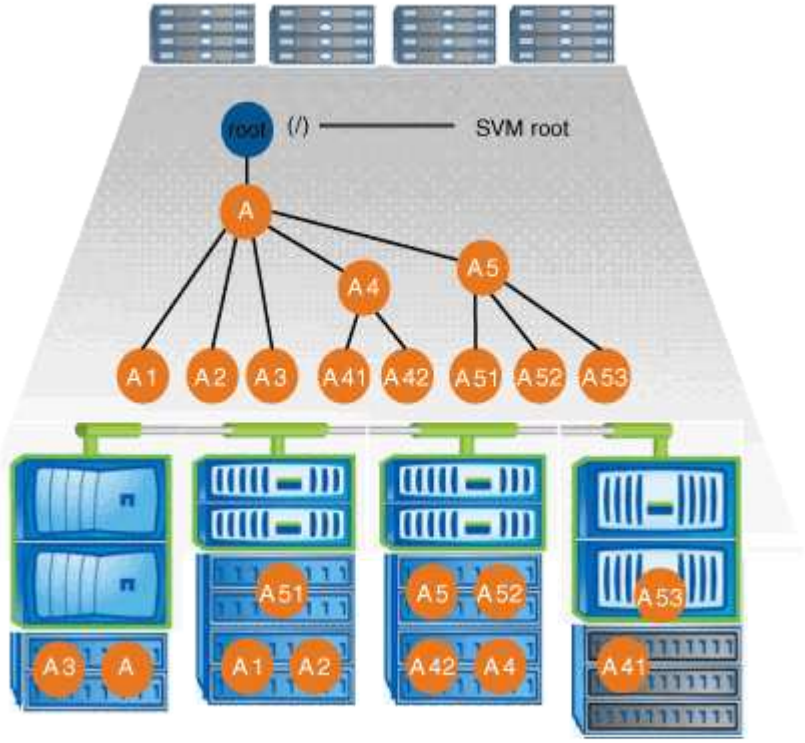
ネームスペースの最上位は常にルートボリュームであり、スラッシュ（ / ）で表されます。ルートの下位のネームスペースアーキテクチャは、次の 3 つの基本カテゴリに分類されます。

- ネームスペースのルートへのジャンクションポイントを 1 つ備えた単一のブランチツリー

- ネームスペースのルートへのジャンクションポイントを複数備えた複数分岐ツリー
- 複数のスタンドアロンボリュームがそれぞれ、ネームスペースのルートへの個別のジャンクションポイントを備えています

単一分岐ツリーを使用するネームスペース

単一分岐のツリーを使用するアーキテクチャには、 SVM ネームスペースのルートへの単一の挿入ポイントがあります。単一の挿入ポイントは、結合されたボリュームまたはルートの下のディレクトリのどちらかになります。それ以外のすべてのボリュームは、単一の挿入ポイントの下のジャンクションポイント（ボリュームまたはディレクトリ）でマウントされます。

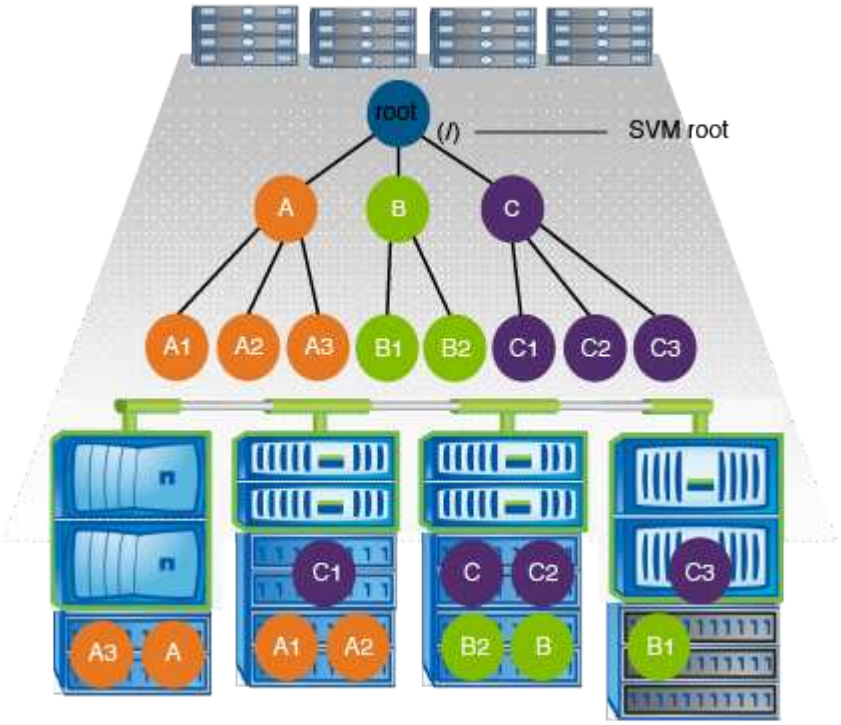


たとえば、上記のネームスペースアーキテクチャを使用する標準的なボリュームジャンクション構成は、すべてのボリュームが単一の挿入ポイントの下で結合された以下のような構成になります。これは「 `d ATA` 」というディレクトリです。

```
                        Junction                          Junction
Vserver Volume          Active   Junction Path            Path Source
------- ------------ -------- -------------------   -----------
vs1     corp1        true     /data/dir1/corp1      RW_volume
vs1     corp2        true     /data/dir1/corp2      RW_volume
vs1     data1        true     /data/data1           RW_volume
vs1     eng1         true     /data/data1/eng1      RW_volume
vs1     eng2         true     /data/data1/eng2      RW_volume
vs1     sales        true     /data/data1/sales     RW_volume
vs1     vol1         true     /data/vol1            RW_volume
vs1     vol2         true     /data/vol2            RW_volume
vs1     vol3         true     /data/vol3            RW_volume
vs1     vs1_root     -        /                     -
```

複数分岐ツリーを使用するネームスペース

複数分岐のツリーを使用するネームスペースには、 SVM ネームスペースのルートへの複数の挿入ポイントがあります。挿入ポイントは、ルート直下で結合されたボリュームまたはディレクトリのどちらかになります。それ以外のすべてのボリュームは、挿入ポイントの下のジャンクションポイント（ボリュームまたはディレクトリ）でマウントされます。

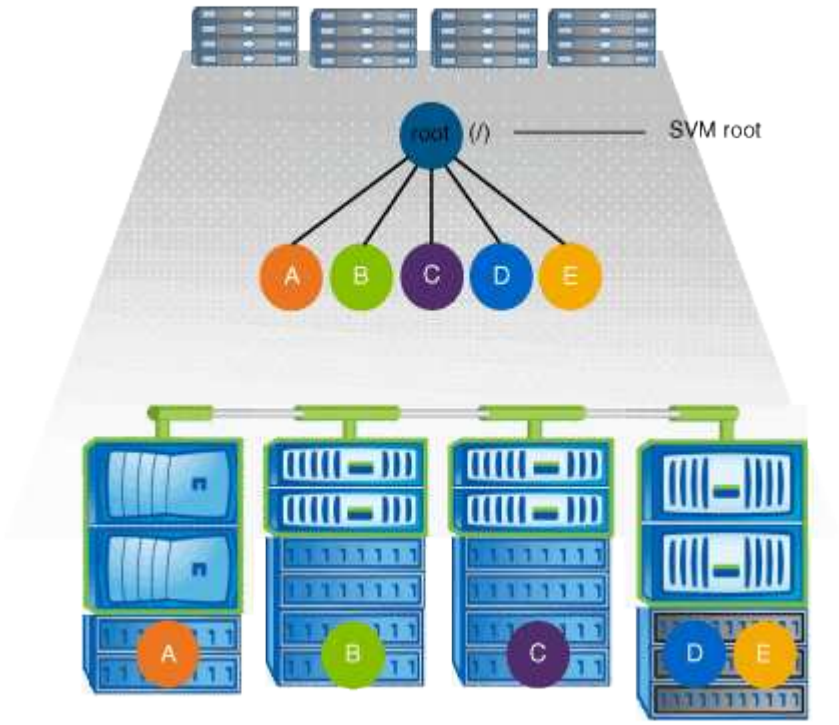


たとえば、上記のネームスペースアーキテクチャを使用する標準的なボリュームジャンクション構成は、SVM のルートボリュームへの 3 つの挿入ポイントがある以下のような構成になります。2 つの挿入ポイントは、「 `d ata" 」と「 projects' 」という名前のディレクトリです。挿入ポイントの 1 つは「 audit 」という名前の結合されたボリュームです。

```
                      Junction                          Junction
Vserver Volume        Active   Junction Path            Path Source
------- ------------ -------- -------------------      -----------
vs1     audit        true     /audit                   RW_volume
vs1     audit_logs1  true     /audit/logs1             RW_volume
vs1     audit_logs2  true     /audit/logs2             RW_volume
vs1     audit_logs3  true     /audit/logs3             RW_volume
vs1     eng          true     /data/eng                RW_volume
vs1     mktg1        true     /data/mktg1              RW_volume
vs1     mktg2        true     /data/mktg2              RW_volume
vs1     project1     true     /projects/project1       RW_volume
vs1     project2     true     /projects/project2       RW_volume
vs1     vs1_root     -        /                        -
```

複数のスタンドアロンボリュームを含むネームスペース

スタンドアロンボリュームを使用するアーキテクチャでは、すべてのボリュームに SVM ネームスペースのルートへの挿入ポイントがありますが、それらのボリュームは別のボリュームの下でジャンクションされません。各ボリュームは一意のパスを持ち、ルート直下で結合されているか、ルートより下のディレクトリで結合されています。



たとえば、上記のネームスペースアーキテクチャを使用する標準的なボリュームジャンクション構成は、SVM のルートボリュームへの 5 つの挿入ポイントがあり、それぞれが 1 つのボリュームへのパスを表す以下のような構成になります。

```
                      Junction                        Junction
Vserver Volume        Active   Junction Path          Path Source
------- ------------ -------- -------------------    -----------
vs1     eng           true     /eng                   RW_volume
vs1     mktg          true     /vol/mktg              RW_volume
vs1     project1      true     /project1              RW_volume
vs1     project2      true     /project2              RW_volume
vs1     sales         true     /sales                 RW_volume
vs1     vs1_root      -        /                      -
```

ONTAP によるファイルアクセスの制御方法

ONTAP によるファイルアクセスの制御の概要

ONTAP は、指定された認証ベースおよびファイルベースの制限に従って、ファイルアクセスを制御します。

クライアントがファイルにアクセスするためにストレージシステムに接続するとき、 ONTAP は 2 つのタスクを実行する必要があります。

- 認証

  ONTAP は、信頼できるソースで ID を検証して、クライアントを認証する必要があります。また、クライアントの認証タイプは、エクスポートポリシーの設定時にクライアントがデータにアクセスできるかどうかの判断に使用できる方法の 1 つです（ CIFS の場合は省略可能）。

- 承認

  ONTAP は、ユーザのクレデンシャルとファイルまたはディレクトリに設定されている権限を比較し、提供するアクセスのタイプ（ある場合）を判別することで、ユーザを許可する必要があります。

ファイルアクセス制御を適切に管理するため、 ONTAP は、 NIS 、 LDAP 、および Active Directory サーバなどの外部サービスと通信します。CIFS または NFS を使用するストレージシステムのファイルアクセスを設定するには、 ONTAP の環境に応じて、サービスを適切に設定する必要があります。

認証ベースの制限

認証ベースの制限を使用すると、 Storage Virtual Machine （ SVM ）に接続できるクライアントマシンおよびユーザを指定できます。

ONTAP は、 UNIX サーバおよび Windows サーバの両方からの Kerberos 認証をサポートします。

ファイルベースの制限

ONTAP では、 3 つのレベルのセキュリティを評価して、 SVM 上にあるファイルおよびディレクトリに対して要求された処理を実行する権限がエンティティにあるかどうかを判断します。アクセスは、 3 つのセキュリティレベルの評価後に有効な権限によって判

断されます。

どのストレージオブジェクトにも、最大 3 種類のセキュリティレイヤを含めることができます。

- エクスポート（ NFS ）および共有（ SMB ）セキュリティ

  指定された NFS エクスポートまたは SMB 共有へのエクスポートおよび共有セキュリティ環境クライアントアクセス管理者権限を持つユーザは、 SMB クライアントと NFS クライアントからエクスポートおよび共有レベルのセキュリティを管理できます。

- ストレージレベルのアクセス保護のファイルおよびディレクトリセキュリティ

  ストレージレベルのアクセス保護セキュリティ環境 SVM ボリュームへの SMB および NFS クライアントアクセスNTFS のアクセス権のみがサポートされています。ONTAP で、ストレージレベルのアクセス保護が適用されているボリューム上のデータにアクセスする UNIX ユーザのセキュリティチェックを行うには、 UNIX ユーザがボリュームを所有する SVM 上の Windows ユーザにマッピングされている必要があります。

  > NFS または SMB クライアントからファイルまたはディレクトリのセキュリティ設定を表示した場合、ストレージレベルのアクセス保護セキュリティは表示されません。システム（ Windows または UNIX ）管理者であっても、ストレージレベルのアクセス保護セキュリティをクライアントから取り消すことはできません。

- NTFS 、 UNIX 、および NFSv4 のネイティブのファイルレベルのセキュリティ

  ストレージオブジェクトを表すファイルやディレクトリには、ネイティブのファイルレベルのセキュリティが存在します。ファイルレベルのセキュリティはクライアントから設定できます。ファイル権限は、データへのアクセスに SMB と NFS のどちらを使用するかに関係なく有効です。

ONTAPによるNFSクライアント認証の処理

ONTAP による NFS クライアント認証の処理の概要

NFS クライアントから SVM 上のデータにアクセスするためには、 NFS クライアントが正しく認証されている必要があります。ONTAP では、 UNIX クレデンシャルを設定されたネームサービスに照らしてチェックすることで、そのクライアントを認証します。

NFS クライアントが SVM に接続すると、 ONTAP は、 SVM のネームサービス設定に応じて複数のネームサービスをチェックし、そのユーザの UNIX クレデンシャルを取得します。ONTAP でチェックできるのは、ローカルの UNIX アカウント、 NIS ドメイン、および LDAP ドメインのクレデンシャルです。ONTAP がユーザを認証できるように、このうちの少なくとも 1 つを設定しておく必要があります。複数 ONTAP のネームサービスと検索順序を指定できます。

UNIX のボリュームセキュリティ形式のみを使用する NFS 環境の場合、この設定だけで NFS クライアントから接続するユーザが認証され、適切なファイルアクセスが提供されます。

mixed、NTFS、またはunifiedのボリュームセキュリティ形式を使用している場合、ONTAPがUNIXユーザをWindowsドメインコントローラで認証するためにはSMBユーザ名を取得する必要があります。これには、ローカルのUNIXアカウントまたはLDAPドメインを使用して個 々 のユーザをマッピングするか、代わりにデフォルトのSMBユーザを使用します。ONTAPが検索するネームサービスの種類と検索順序を指定することも、デフォルトのSMBユーザを指定することもできます。

ONTAP でのネームサービスの使用方法

ONTAP は、ネームサービスを使用してユーザおよびクライアントに関する情報を取得します。ONTAP は、ストレージシステム上でデータにアクセスしたりストレージシステムを管理したりするユーザの認証や、混在環境でのユーザクレデンシャルのマッピングを行うために、この情報を使用します。

ストレージシステムを設定するときに、 ONTAP が認証用のユーザクレデンシャルを取得するために使用するネームサービスを指定する必要があります。ONTAP では、次のネームサービスをサポートしています。

- ローカルユーザ（ファイル）
- 外部 NIS ドメイン（ NIS ）
- 外部LDAPドメイン（LDAP）

を使用します `vserver services name-service ns-switch` ネットワーク情報を検索するソースとソースの検索順序をSVMに設定するコマンドファミリー。これらのコマンドは、と同等の機能を提供します `/etc/nsswitch.conf` UNIXシステム上のファイル。

NFS クライアントが SVM に接続すると、 ONTAP は指定されたネームサービスをチェックして、ユーザの UNIX クレデンシャルを取得します。ネームサービスが正しく設定されていて ONTAP が UNIX クレデンシャルを取得できる場合、 ONTAP はユーザの認証に成功します。

mixed セキュリティ形式の環境では、 ONTAP によるユーザクレデンシャルのマッピングが必要になる場合があります。ONTAP がユーザクレデンシャルを適切にマッピングできるようにするには、環境のネームサービスを適切に設定する必要があります。

ONTAP は、 SVM 管理者アカウントの認証にもネームサービスを使用します。ネームサービススイッチを設定または変更する際にはこの点を念頭に置いて、 SVM 管理者アカウントの認証を誤って無効にしないようにする必要があります。SVM管理ユーザの詳細については、を参照してください "管理者認証と RBAC"。

ONTAP による **NFS** クライアントからの **SMB** ファイルアクセスの許可方法

ONTAP では、 NTFS （ Windows NT ファイルシステム）のセキュリティセマンティクスを利用して、 NTFS アクセス権によるファイルへのアクセス権が、 NFS クライアント上の UNIX ユーザにあるかどうかが判別されます。

ONTAP では、ユーザの UNIX User ID （ UID ； UNIX ユーザ ID ）から変換された SMB クレデンシャルを使用して、ファイルに対するユーザのアクセス権の有無が確認されます。SMB クレデンシャルは、通常はユーザの Windows ユーザ名であるプライマリ Security Identifier （ SID ；セキュリティ識別子）と、ユーザがメンバーとなっている Windows グループに対応する 1 つ以上のグループ SID で構成されています。

ONTAP で UNIX UID を SMB クレデンシャルへ変換するときに要する時間は、数十ミリ秒から数百ミリ秒です。これは、この変換処理にドメインコントローラへの問い合わせも含まれるためです。ONTAP は UID を SMB クレデンシャルにマッピングします。このマッピングはクレデンシャルキャッシュ内に入力されるので、変換によって発生する検証時間が短縮されます。

NFS クレデンシャルキャッシュの仕組み

NFS ユーザがストレージシステム上の NFS エクスポートへのアクセスを要求すると、 ONTAP は、ユーザの認証を行うために外部ネームサーバまたはローカルファイルからユ

ーザクレデンシャルを取得する必要があります。その後、 ONTAP は、以降の参照用にこれらのクレデンシャルを内部のクレデンシャルキャッシュに格納します。NFS クレデンシャルキャッシュの仕組みを理解しておくと、パフォーマンスおよびアクセスに関する潜在的な問題に対処できます。

クレデンシャルキャッシュがないと、 ONTAP ユーザは NFS ユーザからアクセスが要求されるたびにネームサービスを照会しなければなりません。多数のユーザがアクセスする使用頻度の高いストレージシステムでは、こうした状況がすぐに深刻なパフォーマンス上の問題につながり、不必要な遅延や、場合によっては NFS クライアントアクセスの拒否さえ引き起こす可能性があります。

クレデンシャルキャッシュがあれば、 ONTAP は取得したユーザクレデンシャルをあらかじめ決められた期間だけ格納しておき、同じ NFS クライアントから再び要求があっても迅速かつ簡単にアクセスすることができます。この方法には、次の利点があります。

- 外部ネームサーバ（ NIS や LDAP など）への要求の処理を減らすことで、ストレージシステムの負荷が軽減されます。
- 外部ネームサーバに送信する要求を減らすことで、外部ネームサーバの負荷が軽減されます。
- ユーザの認証を行う前に外部ソースからクレデンシャルを取得するための待ち時間をなくすことで、ユーザアクセスが高速になります。

ONTAP は、受理されたクレデンシャルと拒否されたクレデンシャルの両方をクレデン受理されたクレデンシャルとは、ユーザが認証されてアクセス権を付与されたこと拒否されたクレデンシャルとは、ユーザが認証されずにアクセスが拒否されたことを意味します

デフォルトでは、 ONTAP は受理されたクレデンシャルを 24 時間保存します。つまり、ユーザの最初の認証から 24 時間は、そのユーザからのすべてのアクセス要求で ONTAP はキャッシュされたクレデンシャルを使用します。24 時間後にそのユーザからアクセスが要求された場合は、最初からやり直しになります。 ONTAP はキャッシュされたクレデンシャルを破棄し、適切なネームサービスソースから再びクレデンシャルを取得します。それまでの 24 時間にネームサーバ上でクレデンシャルが変更された場合、 ONTAP は、次の 24 時間での使用に備えて、更新されたクレデンシャルをキャッシュします。

デフォルトでは、 ONTAP は拒否されたクレデンシャルを 2 時間保存します。つまり、ユーザに対する最初のアクセス拒否から 2 時間は、そのユーザからのすべてのアクセス要求を ONTAP は拒否し続けます。2 時間後にそのユーザからアクセスが要求された場合は、最初からやり直しになります。 ONTAP は適切なネームサービスソースから再びクレデンシャルを取得します。それまでの 2 時間にネームサーバ上でクレデンシャルが変更された場合、 ONTAP は、次の 2 時間での使用に備えて、更新されたクレデンシャルをキャッシュします。

NAS ネームスペース内でデータボリュームを作成および管理します

ジャンクションポイントを指定してデータボリュームを作成します

ジャンクションポイントはデータボリュームの作成時に指定できます。作成したボリュームは、ジャンクションポイントに自動的にマウントされ、 NAS アクセス用の設定にすぐに使用できます。

作業を開始する前に

- ボリュームを作成するアグリゲートがすでに存在している必要があります。

- ONTAP 9.13.1以降では、容量分析とアクティビティ追跡を有効にしてボリュームを作成できます。容量またはアクティビティトラッキングを有効にするには、を問題します `volume create` コマンドにを指定します `-analytics-state` または `-activity-tracking-state` をに設定します `on`。

  容量分析とアクティビティ追跡の詳細については、を参照してください File System Analytics を有効にします。

> ジャンクションパスに次の文字を使用することはできません。 * # <> < | ? \

[+] また、ジャンクションパスの長さは 255 文字以下にする必要があります。

手順

1. ジャンクションポイントを指定してボリュームを作成します。

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
   {ntfs|unix|mixed} -junction-path junction_path
   ```

   ジャンクションパスはルート（ / ）で始まる必要があり、ディレクトリおよび結合されたボリュームを含むことができます。ジャンクションパスにボリュームの名前を含める必要はありません。ジャンクションパスはボリューム名に依存しません。

   ボリュームのセキュリティ形式の指定は任意です。セキュリティ形式を指定しない場合、 ONTAP は、Storage Virtual Machine （ SVM ）のルートボリュームに適用されている形式と同じセキュリティ形式を使用してボリュームを作成します。ただし、ルートボリュームのセキュリティ形式が、作成するデータボリュームには適切でないセキュリティ形式である場合もあります。トラブルシューティングが困難なファイルアクセスの問題を最小限に抑えるため、ボリュームの作成時にセキュリティ形式を指定することを推奨します。

   ジャンクションパスでは大文字と小文字が区別されません。 `/ENG` はと同じです `/eng`。CIFS 共有を作成する場合、 Windows では、ジャンクションパスがあたかも大文字と小文字の区別があるかのように扱われます。たとえば、ジャンクションがの場合などです `/ENG`SMB共有のパスはで始まる必要があります `/ENG`ではありません `/eng`。

   データボリュームのカスタマイズに使用できるオプションのパラメータが多数用意されています。これらの機能の詳細については、のマニュアルページを参照してください `volume create` コマンドを実行します

2. 目的のジャンクションポイントでボリュームが作成されたことを確認します。

   ```
   volume show -vserver vserver_name -volume volume_name -junction
   ```

例

次の例は、ジャンクションパスがである「home4」という名前のボリュームをSVM vs1上に作成します `/eng/home`：

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                   Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

ジャンクションポイントを指定せずにデータボリュームを作成

ジャンクションポイントを指定せずにデータボリュームを作成できます。作成したボリュームは自動的にはマウントされず、 NAS アクセス用の設定に使用することはできません。ボリュームの SMB 共有または NFS エクスポートを設定する前に、ボリュームをマウントする必要があります。

作業を開始する前に

- ボリュームを作成するアグリゲートがすでに存在している必要があります。
- ONTAP 9.13.1以降では、容量分析とアクティビティ追跡を有効にしてボリュームを作成できます。容量またはアクティビティトラッキングを有効にするには、を問題します `volume create` コマンドにを指定します `-analytics-state` または `-activity-tracking-state` をに設定します `on`。

  容量分析とアクティビティ追跡の詳細については、を参照してください File System Analytics を有効にします。

手順

1. 次のコマンドを使用して、ジャンクションポイントが設定されていないボリュームを作成します。

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
   {ntfs|unix|mixed}
   ```

   ボリュームのセキュリティ形式の指定は任意です。セキュリティ形式を指定しない場合、 ONTAP は、Storage Virtual Machine （ SVM ）のルートボリュームに適用されている形式と同じセキュリティ形式を使用してボリュームを作成します。ただし、ルートボリュームのセキュリティ形式が、データボリュームには適切でないセキュリティ形式である場合もあります。トラブルシューティングが困難なファイルアクセスの問題を最小限に抑えるため、ボリュームの作成時にセキュリティ形式を指定することを推奨します。

   データボリュームのカスタマイズに使用できるオプションのパラメータが多数用意されています。これらの機能の詳細については、のマニュアルページを参照してください `volume create` コマンドを実行します

2. ジャンクションポイントが設定されていないボリュームが作成されたことを確認します。

   ```
   volume show -vserver vserver_name -volume volume_name -junction
   ```

例

次の例は、ジャンクションポイントにマウントされない「 sales 」という名前のボリュームを SVM vs1 上に作成します。

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                      Junction                 Junction
Vserver   Volume      Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data        true     /data           RW_volume
vs1       home4       true     /eng/home       RW_volume
vs1       vs1_root    -        /               -
vs1       sales       -        -               -
```

NAS ネームスペース内の既存のボリュームをマウントまたはアンマウントします

Storage Virtual Machine （ SVM ）ボリュームに格納されたデータへの NAS クライアントアクセスを設定するには、ボリュームが NAS ネームスペースにマウントされている必要があります。現在マウントされていないボリュームは、ジャンクションポイントにマウントできます。ボリュームはアンマウントすることもできます。

このタスクについて

ボリュームをアンマウントしてオフラインにすると、アンマウントしたボリュームのネームスペース内に含まれていたジャンクションポイントのあるボリューム内のデータも含め、ジャンクションポイント内のすべてのデータにNASクライアントからアクセスできなくなります。

> NAS クライアントからのボリュームへのアクセスを中止するには、ボリュームを単純にアンマウントするだけでは不十分です。ボリュームをオフラインにするか、クライアント側のファイルハンドルキャッシュを確実に無効にするためのその他の手順を実行する必要があります。詳細については、次の技術情報アーティクルを参照してください。
>
> "ONTAP のネームスペースから NFSv3 クライアントを削除しても、ボリュームにアクセスできるようになります"

ボリュームをアンマウントしてオフラインにしても、そのボリューム内のデータは失われません。また、既存のボリュームエクスポートポリシーおよびボリュームまたはディレクトリ上に作成された SMB 共有、およびアンマウントされたボリューム内のジャンクションポイントは保持されます。アンマウントしたボリュームを再マウントすれば、 NAS クライアントは既存のエクスポートポリシーと SMB 共有を使用してボリューム内のデータにアクセスできるようになります。

手順

1. 必要な操作を実行します。

状況	入力するコマンド
ボリュームをマウント	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`

ボリュームをアンマウントします	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. ボリュームが目的のマウント状態になっていることを確認します。

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

例

次の例は、SVM「vs1」にある「sales」という名前のボリュームをジャンクションポイント「/sales」にマウントします。

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

次の例は、SVM「vs1」にある「data」という名前のボリュームをアンマウントしてオフラインにします。

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

ボリュームマウントポイントとジャンクションポイントに関する情報を表示します

Storage Virtual Machine （ SVM ）のマウントボリューム、およびボリュームがマウントされているジャンクションポイントに関する情報を表示できます。また、ジャンクションポイントにマウントされていないボリュームを確認することもできます。この情報を使用して、 SVM ネームスペースを理解し、管理することができます。

ステップ

1. 必要な操作を実行します。

表示する項目	入力するコマンド
SVM のマウントされたボリュームとマウントされていないボリュームに関する概要情報	`volume show -vserver` *`vserver_name`* `-junction`
SVM のマウントされたボリュームとマウントされていないボリュームに関する詳細情報	`volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-instance`
SVM のマウントされたボリュームとマウントされていないボリュームに関する特定の情報	a. 必要に応じて、の有効なフィールドを表示できます `-fields` パラメータを指定するには、次のコマンドを使用します。 `volume show -fields ?` b. を使用して、必要な情報を表示します `-fields` パラメータ： `volume show -vserver` *`vserver_name`* `-fields` *`fieldname`*`,…`

例

次の例は、 SVM vs1 のマウントされたボリュームとマウントされていないボリュームの概要を表示します。

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

次の例は、 SVM vs2 上に配置されたボリュームの指定したフィールドに関する情報を表示します。

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -            -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /            -
node3
```

セキュリティ形式を設定する

セキュリティ形式がデータアクセスに与える影響

セキュリティ形式とその影響とは

セキュリティ形式には、 UNIX 、 NTFS 、 mixed 、および unified の 4 種類があり、セキュリティ形式ごとにデータに対する権限の処理方法が異なります。目的に応じて適切なセキュリティ形式を選択できるように、それぞれの影響について理解しておく必要があります。

セキュリティ形式はデータにアクセスできるクライアントの種類には影響しないことに注意してください。セキュリティ形式で決まるのは、データアクセスの制御に ONTAP で使用される権限の種類と、それらの権限を変更できるクライアントの種類だけです。

たとえば、ボリュームで UNIX セキュリティ形式を使用している場合でも、 ONTAP はマルチプロトコルに対応しているため、 SMB クライアントから引き続きデータにアクセスできます（認証と許可が適切な場合）。ただし、 ONTAP では、 UNIX クライアントのみが標準のツールを使用して変更できる UNIX 権限が使用されます。

セキュリティ形式	権限を変更できるクライアント	クライアントが使用できる権限	有効になるセキュリティ形式	ファイルにアクセスできるクライアント
「 UNIX 」	NFS	NFSv3 モードビット	「 UNIX 」	NFS と SMB
		NFSv4.x ACL		
NTFS	SMB	NTFS ACL	NTFS	
混在	NFS または SMB	NFSv3 モードビット	「 UNIX 」	
		NFSv4.x ACL		
		NTFS ACL	NTFS	
統合： （ONTAP 9.4 以前のリリースでは、Infinite Volume のみ）。	NFS または SMB	NFSv3 モードビット	「 UNIX 」	
		NFSv4.1 ACL		
		NTFS ACL	NTFS	

FlexVol ボリュームでは、 UNIX 、 NTFS 、および mixed のセキュリティ形式がサポートされます。セキュリティ形式が mixed または unified の場合は、ユーザがセキュリティ形式を各自設定するため、権限を最後に変更したクライアントの種類によって有効になる権限が異なります。権限を最後に変更したクライアントが NFSv3 クライアントの場合、権限は UNIX NFSv3 モードビットになります。最後のクライアントが NFSv4 クライアントの場合、権限は NFSv4 ACL になります。最後のクライアントが SMB クライアントの場合、権限は Windows NTFS ACL になります。

unified セキュリティ形式は、 Infinite Volume でのみ使用できます。 Infinite Volume は、 ONTAP 9.5 以降のリリースではサポートされなくなりました。詳細については、を参照してください FlexGroup ボリュームの管理の概要。

ONTAP 9.2以降では、 `show-effective-permissions` パラメータをに設定します `vserver security file-directory` コマンドを使用すると、指定したファイルまたはフォルダパスに対してWindowsユーザまたはUNIXユーザに付与されている有効な権限を表示できます。また、オプションのパラメータも指定します `-share-name` 有効な共有権限を表示できます。

> ONTAP で、最初にデフォルトのファイル権限がいくつか設定されます。デフォルトでは、 UNIX 、 mixed 、および unified のセキュリティ形式のボリュームにあるデータについては、セキュリティ形式は UNIX 、権限の種類は UNIX モードビット（特に指定しないかぎり 0755 ）が有効になります。これは、デフォルトのセキュリティ形式で許可されたクライアントで設定するまで変わりません。NTFS セキュリティ形式のボリュームにあるデータについては、デフォルトで NTFS セキュリティ形式が有効になり、すべてのユーザにフルコントロール権限を許可する ACL が割り当てられます。

セキュリティ形式を設定する場所とタイミング

セキュリティ形式は、 FlexVol （ルートボリュームとデータボリュームの両方）および qtree で設定できます。セキュリティ形式は、作成時に手動で設定することも、自動的に継承することも、あとで変更することもできます。

SVM で使用するセキュリティ形式を決定します

ボリュームで使用するセキュリティ形式を決定するには、 2 つの要素を考慮する必要があります。第 1 の要素は、ファイルシステムを管理する管理者のタイプです。第 2 の要

素は、ボリューム上のデータにアクセスするユーザまたはサービスのタイプです。

ボリュームのセキュリティ形式を設定するときは、最適なセキュリティ形式を選択して権限の管理に関する問題を回避するために、環境のニーズを考慮する必要があります。決定時には次の点を考慮すると役立ちます。

セキュリティ形式	以下の場合に選択
「 UNIX 」	• ファイルシステムが UNIX 管理者によって管理される。 • ユーザの大半が NFS クライアントである。 • データにアクセスするアプリケーションで、サービスアカウントとして UNIX ユーザが使用される。
NTFS	• ファイルシステムは Windows 管理者によって管理されます。 • ユーザの大部分がSMBクライアントです。 • データにアクセスするアプリケーションで、サービスアカウントとして Windows ユーザが使用される。
混在	• ファイルシステムが UNIX 管理者と Windows 管理者の両方によって管理され、ユーザが NFS クライアントと SMB クライアントの両方で構成される。

セキュリティ形式の継承の仕組み

新しい FlexVol または qtree の作成時にセキュリティ形式を指定しない場合、セキュリティ形式はさまざまな方法で継承されます。

セキュリティ形式は、次のように継承されます。

- FlexVol ボリュームは、そのボリュームを含む SVM のルートボリュームのセキュリティ形式を継承します。
- qtree は、その qtree を含む FlexVol ボリュームのセキュリティ形式を継承します。
- ファイルまたはディレクトリは、そのファイルまたはディレクトリを含む FlexVol ボリュームまたは qtree のセキュリティ形式を継承します。

ONTAP による **UNIX** アクセス権の維持方法

UNIX アクセス権を現在持っている FlexVol ボリューム内のファイルが Windows アプリケーションによって編集および保存されても、 ONTAP は UNIX アクセス権を維持できます。

Windows クライアントのアプリケーションは、ファイルを編集して保存するときに、ファイルのセキュリティプロパティを読み取り、新しい一時ファイルを作成し、それらのプロパティを一時ファイルに適用してから、一時ファイルに元のファイル名を付けます。

セキュリティプロパティのクエリを実行すると、 Windows クライアントは、 UNIX アクセス権を正確に表す構築済み ACL を受け取ります。この構築済み ACL は、 Windows アプリケーションによってファイルが更新されるときにファイルの UNIX アクセス権を維持し、生成されたファイルが同じ UNIX アクセス権を持つようにするためだけに使用されます。ONTAP は、構築済み ACL を使用して NTFS ACL を設定しません。

SVM 上の mixed セキュリティ形式のボリュームまたは qtree に含まれるファイルまたはフォルダの UNIX アクセス権を操作する場合は、 Windows クライアントのセキュリティタブを使用できます。また、 Windows ACL を照会および設定できるアプリケーションを使用することもできます。

- UNIX アクセス権の変更

  Windows のセキュリティタブを使用して、 mixed セキュリティ形式のボリュームまたは qtree の UNIX アクセス権を表示および変更できます。メインの [Windows Security] タブを使用して UNIX アクセス権を変更する場合は、編集する既存の ACE を削除してから（モードビットを 0 に設定）、変更を行う必要があります。または、高度なエディタを使用して権限を変更することもできます。

  モードのアクセス権を使用している場合は、リストされた UID 、 GID 、およびその他（コンピュータにアカウントを持つその他すべてのユーザ）のモードアクセス権を直接変更できます。たとえば、表示された UID に r-x のアクセス権が設定されている場合、この UID のアクセス権を rwx に変更できます。

- UNIX アクセス権を NTFS アクセス権に変更しています

  Windows のセキュリティタブを使用して、ファイルおよびフォルダのセキュリティ形式が UNIX 対応である mixed 型セキュリティ形式のボリュームまたは qtree 上で、 UNIX セキュリティオブジェクトを Windows セキュリティオブジェクトに置き換えることができます。

  適切な Windows のユーザおよびグループのオブジェクトに置き換える前に、リストされている UNIX アクセス権のエントリをすべて削除しておく必要があります。次に、 Windows のユーザおよびグループのオブジェクトに NTFS ベースの ACL を設定します。すべての UNIX セキュリティオブジェクトを削除し、 Windows のユーザおよびグループのみを mixed セキュリティ形式のボリュームまたは qtree 上のファイルまたはフォルダに追加すると、ファイルまたはフォルダのセキュリティ形式が UNIX から NTFS へ変換されます。

  フォルダの権限を変更する場合、 Windows のデフォルトの動作では、すべてのサブフォルダとファイルにこれらの変更が反映されます。したがって、セキュリティ形式の変更をすべての子フォルダ、サブフォルダ、およびファイルに反映したくない場合は、反映する範囲を希望の範囲に変更する必要があります。

SVM ルートボリュームのセキュリティ形式を設定する

Storage Virtual Machine （ SVM ）のルートボリューム上のデータに使用するアクセス権のタイプを決定するには、 SVM ルートボリュームのセキュリティ形式を設定します。

手順

1. を使用します `vserver create` コマンドにを指定します `-rootvolume-security-style` セキュリティ形式を定義するパラメータ。

   ルートボリュームのセキュリティ形式に指定できるオプションは、です `unix`、 `ntfs``または `mixed`。

2. 作成した SVM のルートボリュームセキュリティ形式を含む設定を表示して確認します。

   ```
   vserver show -vserver vserver_name
   ```

FlexVol ボリュームのセキュリティ形式を設定する

Storage Virtual Machine （ SVM ）の FlexVol 上のデータに使用するアクセス権のタイプを決定するには、 FlexVol のセキュリティ形式を設定します。

手順

1. 次のいずれかを実行します。

FlexVol ボリュームの状況	使用するコマンド
はまだ存在しません	`volume create` を含めます `-security-style` セキュリティ形式を指定するパラメータ。
はすでに存在します	`volume modify` を含めます `-security-style` セキュリティ形式を指定するパラメータ。

   FlexVol のセキュリティ形式に指定できるオプションは、です `unix`、 `ntfs`または `mixed`。

   FlexVol ボリュームの作成時にセキュリティ形式を指定しない場合、ボリュームはルートボリュームのセキュリティ形式を継承します。

   詳細については、を参照してください `volume create` または `volume modify` コマンド、を参照してください "論理ストレージ管理"。

2. 作成した FlexVol ボリュームのセキュリティ形式を含む設定を表示するには、次のコマンドを入力します。

```
volume show -volume volume_name -instance
```

qtree にセキュリティ形式を設定する

qtree 上のデータに使用するアクセス権のタイプを決定するには、 qtree のセキュリティ形式を設定します。

手順

1. 次のいずれかを実行します。

qtree の有無	使用するコマンド
はまだ存在しません	`volume qtree create` を含めます `-security-style` セキュリティ形式を指定するパラメータ。
はすでに存在します	`volume qtree modify` を含めます `-security-style` セキュリティ形式を指定するパラメータ。

   qtreeセキュリティ形式に指定できるオプションは、です `unix`、 `ntfs`または `mixed`。

   qtreeの作成時にセキュリティ形式を指定しない場合、デフォルトのセキュリティ形式はです `mixed`。

詳細については、を参照してください `volume qtree create` または `volume qtree modify` コマンド、を参照してください "論理ストレージ管理"。

2. 作成したqtreeのセキュリティ形式を含む設定を表示するには、次のコマンドを入力します。 `volume qtree show -qtree *qtree_name* -instance`

NFSを使用したファイルアクセスの設定

NFS の概要を使用したファイルアクセスのセットアップ

クライアントが NFS を使用して Storage Virtual Machine （ SVM ）上のファイルにアクセスできるようにするには、いくつかの手順を実行する必要があります。環境の現在の設定によっては、さらにいくつかの手順を実行することもできます。

クライアントが NFS を使用して SVM のファイルにアクセスできるようにするには、次の作業を行う必要があります。

1. SVM で NFS プロトコルを有効にします。

   クライアントからの NFS 経由のデータアクセスを許可するように SVM を設定する必要があります。

2. SVM に NFS サーバを作成します。

   NFS サーバは、 NFS 経由のファイル提供を可能にする SVM 上の論理エンティティです。NFS サーバを作成し、許可する NFS プロトコルのバージョンを指定する必要があります。

3. SVM でエクスポートポリシーを設定します。

   クライアントがボリュームと qtree を使用できるようにするには、エクスポートポリシーを設定する必要があります。

4. ネットワークおよびストレージの環境に応じて、適切なセキュリティおよびその他の設定を使用して NFS サーバを設定します。

   この手順には、 Kerberos 、 LDAP 、 NIS 、ネームマッピング、ローカルユーザの設定が含まれます。

エクスポートポリシーを使用して NFS アクセスを保護

エクスポートポリシーがボリュームまたは qtree へのクライアントアクセスを制御する仕組み

エクスポートポリシーには、各クライアントアクセス要求を処理する 1 つ以上の _ エクスポートルール _ が含まれています。このプロセスの結果、クライアントアクセスを許可するかどうか、およびアクセスのレベルが決まります。クライアントがデータにアクセスするためには、エクスポートルールを含むエクスポートポリシーが Storage Virtual Machine （ SVM ）上に存在する必要があります。

ボリュームまたは qtree へのクライアントアクセスを設定するには、各ボリュームまたは qtree にポリシーを 1 つ関連付けます。SVM には複数のエクスポートポリシーを含めることができます。これにより、複数のボリュームまたは qtree を含む SVM に対して次の操作を実行できます。

- SVM のボリュームまたは qtree ごとに異なるエクスポートポリシーを割り当て、 SVM の各ボリュームまたは qtree へのクライアントアクセスを個別に制御する。
- SVM の複数のボリュームまたは qtree に同じエクスポートポリシーを割り当て、同一のクライアントアクセス制御を実行する。ボリュームまたは qtree ごとに新しいエクスポートポリシーを作成する必要はありません。

クライアントが適用可能なエクスポートポリシーで許可されていないアクセス要求を行うと、権限拒否のメッセージが表示され、その要求は失敗します。クライアントがエクスポートポリシーのどのルールにも一致しない場合、アクセスは拒否されます。エクスポートポリシーが空の場合は、すべてのアクセスが暗黙的に拒否されます。

エクスポートポリシーは、 ONTAP を実行しているシステム上で動的に変更できます。

SVM のデフォルトのエクスポートポリシー

各 SVM には、ルールが含まれていないデフォルトのエクスポートポリシーが用意されています。SVM 上のデータにクライアントからアクセスできるようにするには、ルールを備えたエクスポートポリシーを用意する必要があります。SVM 内の各 FlexVol にエクスポートポリシーを関連付ける必要があります。

SVMを作成すると、という名前のデフォルトのエクスポートポリシーがストレージシステムによって自動的に作成されます `default` SVMのルートボリュームに対して実行します。SVM 上のデータにクライアントからアクセスできるようにするには、デフォルトのエクスポートポリシーのルールを 1 つ以上作成する必要があります。または、ルールを備えたカスタムのエクスポートポリシーを作成することもできます。デフォルトのエクスポートポリシーは、変更および名前変更は可能ですが、削除することはできません。

SVM 内に FlexVol ボリュームを作成すると、作成されたボリュームには、 SVM のルートボリュームのデフォルトのエクスポートポリシーが関連付けられます。デフォルトでは、 SVM に作成した各ボリュームには、ルートボリュームのデフォルトのエクスポートポリシーが関連付けられます。SVM 内のすべてのボリュームでデフォルトのエクスポートポリシーを使用することも、ボリュームごとに独自のエクスポートポリシーを作成することもできます。複数のボリュームを同じエクスポートポリシーに関連付けることができます。

エクスポートルールの仕組み

エクスポートルールは、エクスポートポリシーの機能要素です。エクスポートルールでは、ボリュームへのクライアントアクセス要求が設定済みの特定のパラメータと照合され、クライアントアクセス要求の処理方法が決定されます。

エクスポートポリシーには、クライアントにアクセスを許可するエクスポートルールが少なくとも 1 つ含まれている必要があります。エクスポートポリシーに複数のルールが含まれている場合、ルールはエクスポートポリシーに表示される順に処理されます。ルールの順序は、ルールインデックス番号によって決まります。ルールがクライアントに一致すると、そのルールの権限が使用され、それ以降のルールは処理されません。一致するルールがない場合、クライアントはアクセスを拒否されます。

次の条件を使用して、クライアントのアクセス権限を決定するようにエクスポートルールを設定できます。

- クライアントが要求の送信に使用するファイルアクセスプロトコル。たとえば、 NFSv4 や SMB などです。
- ホスト名や IP アドレスなどのクライアント識別子。

の最大サイズ `-clientmatch` フィールドは4096文字です。

- Kerberos v5 、 NTLM 、 AUTH_SYS など、クライアントが認証に使用するセキュリティタイプ。

ルールで複数の条件が指定されている場合、クライアントがそれらのすべてに一致しないとルールは適用されません。

> ONTAP 9.3 以降では、エクスポートポリシーの設定チェックをバックグラウンドジョブとして有効にし、すべてのルール違反をエラールールリストに記録することができます。。 `vserver export-policy config-checker` コマンドを実行するとチェッカーが呼び出されて結果が表示され、設定を検証したり、誤ったルールをポリシーから削除したりできます。
>
> このコマンドで検証されるのは、エクスポート設定のホスト名、ネットグループ、匿名ユーザのみです。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアントアクセス要求は NFSv3 プロトコルを使用して送信され、クライアントの IP アドレスは 10.1.17.37 です。

クライアントアクセスプロトコルが一致していても、クライアントの IP アドレスがエクスポートルールで指定されているアドレスとは別のサブネットに属しています。そのため、クライアントは一致しなくなり、このルールはこのクライアントに適用されません。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアントアクセス要求はNFSv4プロトコルを使用して送信され、クライアントのIPアドレスは10.1.16.54です。

クライアントアクセスプロトコルが一致し、クライアントの IP アドレスが指定したサブネット内にあります。そのため、クライアントは一致し、このルールはこのクライアントを環境します。セキュリティタイプに関係なく、クライアントは読み取り / 書き込みアクセス権を取得します。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

クライアント #1 は、 IP アドレスが 10.1.16.207 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、Kerberos v5 で認証されます。

クライアント #2 は、 IP アドレスが 10.1.16.211 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、AUTH_SYS で認証されます。

両方のクライアントで、クライアントアクセスプロトコルと IP アドレスは一致しています。読み取り専用パラメータでは、認証に使用するセキュリティタイプに関係なく、読み取り専用アクセスがすべてのクライアントに許可されています。したがって、両方のクライアントが読み取り専用アクセス権を取得します。ただし、読み取り / 書き込みアクセス権を取得するのはクライアント #1 だけです。これは、認証に承認されたセキュリティタイプ Kerberos v5 を使用したためです。クライアント #2 は読み取り / 書き込みアクセス権を取得できません。

リストにないセキュリティタイプを使用するクライアントを管理します

エクスポートルールのアクセスパラメータに指定されていないセキュリティタイプをクライアントが使用している場合は、オプションを使用して、クライアントへのアクセスを拒否するか、クライアントを匿名ユーザIDにマッピングするかを選択できます `none` にアクセスパラメータを指定します。

クライアントは、別のセキュリティタイプで認証されているか、まったく認証されていない（セキュリティタイプ AUTH_NONE ）場合に、アクセスパラメータで指定されていないセキュリティタイプを使用しているとみなされます。デフォルトでは、クライアントはそのレベルへのアクセスを自動的に拒否されます。ただし、オプションは追加できます `none` をアクセスパラメータに追加します。リストにないセキュリティ形式を使用するクライアントは、拒否されずに匿名ユーザ ID にマッピングされます。。 `-anon` パラメータは、これらのクライアントに割り当てるユーザIDを決定します。に指定されたユーザID `-anon` パラメータは、匿名ユーザに適していると思われる権限が設定されている有効なユーザである必要があります。

に有効な値 `-anon` パラメータの範囲はからです `0` 終了： `65535`。

に割り当てられたユーザ**ID** `-anon`	クライアントアクセス要求の処理結果
`0 - 65533`	クライアントアクセス要求は匿名ユーザ ID にマッピングされ、このユーザに対して設定された権限に応じてアクセスできるようになります。
`65534`	クライアントアクセス要求はユーザ nobody にマッピングされ、このユーザに対して設定されたアクセス権に応じてアクセスできるようになります。これがデフォルトです。

に割り当てられたユーザ**ID** `-anon`	クライアントアクセス要求の処理結果
`65535`	この ID にマッピングされていて、クライアントがセキュリティタイプ AUTH_NONE を使用している場合、クライアントからのアクセス要求は拒否されます。ユーザ ID が 0 のクライアントからのアクセス要求は、この ID にマッピングされ、他のセキュリティタイプをクライアントが使用している場合、拒否されます。

オプションを使用する場合 `none`では、最初に読み取り専用パラメータが処理されることを覚えておくことが重要です。リストにないセキュリティタイプを使用するクライアントのエクスポートルールを設定する際は、次のガイドラインを考慮してください。

読み取り専用にはが含まれます `none`	読み取り/書き込みに含まれます `none`	リストにないセキュリティタイプを使用するクライアントのアクセス結果
いいえ	いいえ	拒否されました
いいえ	はい。	最初に読み取り専用が処理されるため、拒否されました
はい。	いいえ	匿名として読み取り専用です
はい。	はい。	匿名として読み書き可能です

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

クライアント #1 は、 IP アドレスが 10.1.16.207 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、Kerberos v5 で認証されます。

クライアント #2 は、 IP アドレスが 10.1.16.211 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、AUTH_SYS で認証されます。

クライアント #3 は、 IP アドレスが 10.1.16.234 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、認証は行われていません（セキュリティタイプ AUTH_NONE ）。

3 つすべてのクライアントで、クライアントアクセスプロトコルと IP アドレスは一致しています。読み取り専用パラメータでは、読み取り専用アクセスが、 AUTH_SYS で認証された、自身のユーザ ID を持つクライアントに許可されています。読み取り専用パラメータでは、ユーザ ID が 70 の匿名ユーザとしての読み取り

専用アクセスが、他のセキュリティタイプを使用して認証されたクライアントに許可されています。読み取り / 書き込みパラメータでは、読み取り / 書き込みアクセスがすべてのセキュリティタイプに許可されていますが、この場合は、読み取り専用ルールですでにフィルタされている環境クライアントのみが許可されます。

したがって、クライアント #1 とクライアント #3 は、ユーザ ID が 70 の匿名ユーザとしてのみ読み取り / 書き込みアクセス権を取得します。クライアント #2 は、自身のユーザ ID で読み取り / 書き込みアクセス権を取得します。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

クライアント #1 は、 IP アドレスが 10.1.16.207 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、Kerberos v5 で認証されます。

クライアント #2 は、 IP アドレスが 10.1.16.211 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、AUTH_SYS で認証されます。

クライアント #3 は、 IP アドレスが 10.1.16.234 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、認証は行われていません（セキュリティタイプ AUTH_NONE ）。

3 つすべてのクライアントで、クライアントアクセスプロトコルと IP アドレスは一致しています。読み取り専用パラメータでは、読み取り専用アクセスが、 AUTH_SYS で認証された、自身のユーザ ID を持つクライアントに許可されています。読み取り専用パラメータでは、ユーザ ID が 70 の匿名ユーザとしての読み取り専用アクセスが、他のセキュリティタイプを使用して認証されたクライアントに許可されています。読み取り / 書き込みパラメータでは、匿名ユーザとしてのみ読み取り / 書き込みアクセスが許可されています。

したがって、クライアント #1 とクライアント #3 は、ユーザ ID が 70 の匿名ユーザとしてのみ読み取り / 書き込みアクセス権を取得します。クライアント #2 は、自身のユーザ ID で読み取り専用アクセス権を取得しますが、読み取り / 書き込みアクセスは拒否されます。

セキュリティタイプによるクライアントアクセスレベルの決定方法

クライアントの認証に使用されるセキュリティタイプは、エクスポートルールで特別な役割を果たします。クライアントがボリュームまたは qtree にアクセスする際のレベルがセキュリティタイプによってどのように決定されるかについて理解しておく必要があります。

アクセスレベルには、次の 3 つがあります。

1. 読み取り専用です
2. 読み書き可能です
3. superuser （ユーザ ID が 0 のクライアントの場合）

セキュリティタイプに基づくアクセスレベルはこの順序で評価されるため、エクスポートルールでアクセスレベルパラメータを作成するときは、次のルールに従う必要があります。

クライアントに必要なアクセスレベル	クライアントのセキュリティタイプと一致する必要があるアクセスパラメータ
標準ユーザの読み取り専用	読み取り専用です (`-rorule`)
標準ユーザの読み取り / 書き込み	読み取り専用です (`-rorule`）および読み取り/書き込み (`-rwrule`)
スーパーユーザの読み取り専用です	読み取り専用です (`-rorule`）および `-superuser`
スーパーユーザの読み取り / 書き込み	読み取り専用です (`-rorule`）および読み取り/書き込み (`-rwrule`）および `-superuser`

次に、これらの 3 つのアクセスパラメータのそれぞれで有効なセキュリティタイプを示します。

- `any`
- `none`
- `never`

  このセキュリティタイプは、では使用できません `-superuser` パラメータ

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

クライアントのセキュリティタイプを 3 つの各アクセスパラメータと照合したときの結果としては、次の 3 つが考えられます。

クライアントのセキュリティタイプ	クライアント
アクセスパラメータで指定されたタイプと一致する。	独自のユーザ ID を使用して、そのレベルのアクセス権を取得します。
指定したタイプと一致しないが、アクセスパラメータにオプションが指定されている `none`。	で指定されたユーザIDを持つ匿名ユーザとして、そのレベルのアクセス権を取得します `-anon` パラメータ

クライアントのセキュリティタイプ	クライアント
指定したタイプと一致しないため、アクセスパラメータにオプションが指定されていません none。	は、そのレベルのアクセス権を取得しません。これは、には適用されません -superuser パラメータには常にが含まれているためです none 指定されていない場合でも。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- -protocol nfs3
- -clientmatch 10.1.16.0/255.255.255.0
- -rorule any
- -rwrule sys,krb5
- -superuser krb5

クライアント #1 は、 IP アドレスが 10.1.16.207 、ユーザ ID が 0 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、 Kerberos v5 で認証されます。

クライアント #2 は、 IP アドレスが 10.1.16.211 、ユーザ ID が 0 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、 AUTH_SYS で認証されます。

クライアント #3 は、 IP アドレスが 10.1.16.234 、ユーザ ID が 0 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、認証は行われていません（ AUTH_NONE ）。

3 つすべてのクライアントで、クライアントアクセスプロトコルと IP アドレスは一致しています。読み取り専用パラメータでは、セキュリティタイプに関係なく、読み取り専用アクセスがすべてのクライアントに許可されています。読み取り / 書き込みパラメータでは、読み取り / 書き込みアクセスが、 AUTH_SYS または Kerberos v5 で認証された、自身のユーザ ID を持つクライアントに許可されています。スーパーユーザパラメータでは、スーパーユーザアクセスが、 Kerberos v5 で認証された、ユーザ ID が 0 のクライアントに許可されています。

したがって、クライアント #1 は、 3 つすべてのアクセスパラメータに一致するため、スーパーユーザの読み取り / 書き込みアクセス権を取得します。クライアント #2 は、読み取り / 書き込みアクセス権を取得しますが、スーパーユーザアクセス権は取得できません。クライアント #3 は、読み取り専用アクセス権を取得しますが、スーパーユーザアクセス権は取得できません。

スーパーユーザのアクセス要求を管理します

エクスポートポリシーを設定する際には、ストレージシステムがユーザ ID が 0 のクライアントアクセス要求をスーパーユーザとして受信し、それに応じてエクスポートルールを設定する場合に必要な処理を考慮する必要があります。

UNIX の世界では、ユーザ ID 0 のユーザがスーパーユーザと呼ばれ、通常は root と呼ばれます。このユーザにはシステム上で無制限のアクセス権が与えられています。スーパーユーザ権限の使用は、システムやデータセキュリティの侵害などのいくつかの理由によってリスクを伴う可能性があります。

デフォルトでは、 ONTAP はユーザ ID が 0 のクライアントを匿名ユーザにマッピングします。ただし、は指定できます - superuser ユーザIDが0のクライアントの処理方法（セキュリティタイプに応じて）を決定す

るエクスポートルールのパラメータ。で有効なオプションは次のとおりです `-superuser` パラメータ：

- `any`
- `none`

  これは、を指定しない場合のデフォルト設定です `-superuser` パラメータ

- `krb5`
- `ntlm`
- `sys`

ユーザIDが0のクライアントは、に応じて2つの方法で処理されます `-superuser` パラメータ設定：

状況に応じて **-superuser** パラメータおよびクライアントのセキュリティタイプ	クライアント
一致	ユーザ ID 0 でスーパーユーザアクセス権を取得します。
一致しません	で指定されたユーザIDを持つ匿名ユーザとしてアクセスを取得します `-anon` パラメータとその割り当てられた権限。これは、読み取り専用パラメータと読み取り/書き込みパラメータのどちらでオプションが指定されているかに関係ありません `none`。

クライアントがNTFSセキュリティ形式およびのボリュームにアクセスするためにユーザID 0を提示する場合 `-superuser` パラメータはに設定されます `none`ONTAP では、匿名ユーザがネームマッピングを使用して適切なクレデンシャルを取得します。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

クライアント#1は、IPアドレスが10.1.16.207、ユーザIDが746で、NFSv3プロトコルを使用してアクセス要求を送信し、Kerberos v5で認証されます。

クライアント #2 は、 IP アドレスが 10.1.16.211 、ユーザ ID が 0 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、 AUTH_SYS で認証されます。

両方のクライアントで、クライアントアクセスプロトコルと IP アドレスは一致しています。読み取り専用パラメータでは、認証に使用するセキュリティタイプに関係なく、読み取り専用アクセスがすべてのクライアントに許可されています。ただし、読み取り / 書き込みアクセス権を取得するのはクライアント #1 だけです。

これは、認証に承認されたセキュリティタイプ Kerberos v5 を使用したためです。

クライアント #2 は、スーパーユーザアクセス権を取得できません。代わりに、が原因で匿名にマッピングされます `-superuser` パラメータが指定されていません。つまり、デフォルトはです `none` ユーザID 0を匿名に自動的にマッピングします。また、クライアント #2 はセキュリティタイプが読み取り / 書き込みパラメータと一致しなかったため、読み取り専用アクセス権のみを取得します。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

クライアント #1 は、 IP アドレスが 10.1.16.207 、ユーザ ID が 0 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、 Kerberos v5 で認証されます。

クライアント #2 は、 IP アドレスが 10.1.16.211 、ユーザ ID が 0 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、 AUTH_SYS で認証されます。

両方のクライアントで、クライアントアクセスプロトコルと IP アドレスは一致しています。読み取り専用パラメータでは、認証に使用するセキュリティタイプに関係なく、読み取り専用アクセスがすべてのクライアントに許可されています。ただし、読み取り / 書き込みアクセス権を取得するのはクライアント #1 だけです。これは、認証に承認されたセキュリティタイプ Kerberos v5 を使用したためです。クライアント #2 は読み取り / 書き込みアクセス権を取得できません。

このエクスポートルールでは、ユーザ ID が 0 のクライアントにスーパーユーザアクセスが許可されています。クライアント#1は、読み取り専用およびのユーザIDおよびセキュリティタイプと一致するため、スーパーユーザアクセスを取得します `-superuser` パラメータクライアント#2のセキュリティタイプが読み取り/書き込みパラメータまたはと一致しないため、読み取り/書き込みアクセス権もスーパーユーザアクセス権も取得されません `-superuser` パラメータ代わりに、クライアント #2 は匿名ユーザにマッピングされます。この場合、ユーザ ID は 0 です。

ONTAP でのエクスポートポリシーキャッシュの使用方法

システムパフォーマンスを向上するために、 ONTAP はローカルキャッシュを使用してホスト名やネットグループなどの情報を格納します。これにより、 ONTAP は外部ソースから情報を取得するよりも迅速にエクスポートポリシールールを処理できます。キャッシュとは何か、またキャッシュによって何が行われるのかを理解すると、クライアントアクセスに関する問題のトラブルシューティングに役立ちます。

NFS エクスポートへのクライアントアクセスを制御するには、エクスポートポリシーを設定します。各エクスポートポリシーにはルールが含まれており、各ルールにはアクセスを要求しているクライアントに対するマッチングを行うパラメータが含まれています。これらのパラメータの一部では、ドメイン名、ホスト名、ネットグループなどのオブジェクトを解決するために ONTAP が DNS サーバや NIS サーバのような外部ソースと通信する必要があります。

外部ソースとの通信には少し時間がかかります。パフォーマンスを向上させるために、 ONTAP は、各ノード上の複数のキャッシュに情報をローカルに格納して、エクスポートポリシールールオブジェクトの解決にかかる時間を短縮します。

キャッシュ名	保存される情報のタイプ
にアクセスします	対応するエクスポートポリシーへのクライアントのマッピング
名前	対応する UNIX ユーザ ID への UNIX ユーザ名のマッピング
ID	対応する UNIX ユーザ ID および拡張された UNIX グループ ID への UNIX ユーザ ID のマッピング
ホスト	対応する IP アドレスへのホスト名のマッピング
ネットグループ	メンバーの対応する IP アドレスへのネットグループのマッピング
showmount	SVM ネームスペースからエクスポートされたディレクトリのリスト

ONTAP が外部ネームサーバ上の情報を取得してローカルに格納したあとに、環境内の外部ネームサーバ上の情報を変更すると、キャッシュ内の情報が古くなる可能性があります。ONTAP は一定期間の経過後に自動的にキャッシュを更新しますが、有効期限や更新の時期およびアルゴリズムはキャッシュごとに異なります。

キャッシュに古くなった情報が含まれる理由としてもう 1 つ考えられるのは、 ONTAP がキャッシュされた情報の更新を試みたにもかかわらずネームサーバと通信しようとしてエラーが発生した場合です。この場合、ONTAP は、クライアントの中断を避けるために現在ローカルキャッシュに格納されている情報を引き続き使用します。

その結果、成功することが想定されるクライアントアクセス要求が失敗し、エラーとなることが想定されるクライアントアクセス要求が成功する可能性があります。クライアントアクセスに関するこのような問題のトラブルシューティング時には、エクスポートポリシーキャッシュの一部を表示したり、手動でフラッシュしたりできます。

アクセスキャッシュの仕組み

ONTAP は、アクセスキャッシュを使用して、ボリュームまたは qtree へのクライアントアクセス処理に対するエクスポートポリシールール評価の結果を格納します。これにより、クライアントから I/O 要求が送信されるたびにエクスポートポリシールール評価の処理を行う場合よりも、アクセスキャッシュから情報をはるかに短時間で取得できるため、パフォーマンスが向上します。

NFS クライアントがボリュームまたは qtree 上のデータにアクセスするための I/O 要求を送信するたびに、ONTAP はそれぞれの I/O 要求を評価して、その I/O 要求を許可するか拒否するかを決定する必要があります。この評価には、そのボリュームまたは qtree に関連付けられているすべてのエクスポートポリシールールのチェックが伴います。ボリュームまたは qtree へのパスが 1 つ以上のジャンクションポイントと交差してい

る場合は、そのパスに付随する複数のエクスポートポリシーに対してこのチェックの実行が必要になる可能性があります。

なお、この評価は、最初のマウント要求についてだけでなく、読み取り、書き込み、リスト、コピーなどの処理を行う NFS クライアントから送信されたすべての I/O 要求について行われます。

ONTAP が適用可能なエクスポートポリシールールを特定して要求を許可するか拒否するかを決定すると、ONTAP はその情報を格納するためのエントリをアクセスキャッシュ内に作成します。

NFS クライアントが I/O 要求を送信すると、 ONTAP は、そのクライアントの IP アドレス、 SVM の ID 、ターゲットボリュームまたは qtree に関連付けられているエクスポートポリシーを記録したうえで、まずアクセスキャッシュをチェックして一致するエントリがないか確認します。一致するエントリがアクセスキャッシュ内に存在する場合、 ONTAP はそこに格納されている情報を使用して、 I/O 要求を許可または拒否します。一致するエントリが存在しない場合、 ONTAP は先ほど述べたすべての適用可能なポリシールールを評価する通常の処理を行います。

アクティブに使用されていないアクセスキャッシュエントリは更新されません。これにより、外部ネームサーバとの無駄な通信が削減されます。

アクセスキャッシュからの情報の取得は、 I/O 要求のたびにエクスポートポリシールールを評価する全体的な処理よりもずっと高速です。そのため、アクセスキャッシュを使用すると、クライアントアクセスチェックのオーバーヘッドが軽減され、パフォーマンスが大幅に向上します。

アクセスキャッシュパラメータの仕組み

アクセスキャッシュ内のエントリの更新期間を制御するパラメータがいくつかあります。これらのパラメータの仕組みを理解すると、各パラメータを変更してアクセスキャッシュを調整し、パフォーマンスと格納される情報の鮮度のバランスを取ることができます。

アクセスキャッシュには、ボリュームまたは qtree へのアクセスを試みるクライアントに適用される 1 つ以上のエクスポートルールで構成されるエントリが格納されます。これらのエントリは、一定期間格納されたあと、更新されます。更新時間はアクセスキャッシュパラメータによって決定され、アクセスキャッシュエントリのタイプによって異なります。

アクセスキャッシュパラメータは、個々の SVM に対して指定できます。これにより、 SVM のアクセス要件に応じてパラメータを変更できます。アクティブに使用されていないアクセスキャッシュエントリは更新されないため、外部ネームサーバとの無駄な通信が削減されます。

アクセスキャッシュエントリタイプ	説明	更新期間（秒）
正のエントリ	クライアントへのアクセス拒否を発生させなかったアクセスキャッシュエントリです。	最小値： 300 最大値： 86 、 400 デフォルト値は 3,600 です。

負のエントリ	クライアントへのアクセス拒否を発生させたアクセスキャッシュエントリです。	最小：60 最大値： 86 、 400 デフォルト値は 3,600 です。

例

NFS クライアントがクラスタ上のボリュームへのアクセスを試みます。ONTAP は、エクスポートポリシールールに対するクライアントのマッチングを行い、クライアントがエクスポートポリシールール設定に基づいてアクセスを行っていると判断します。ONTAP はエクスポートポリシールールを正のエントリとしてアクセスキャッシュに格納します。デフォルトでは、 ONTAP は、この正のエントリを 1 時間（ 3 、 600 秒）アクセスキャッシュ内に保持したあと、情報を最新の状態にするためにこのエントリを自動的に更新します。

アクセスキャッシュが不必要にいっぱいになるのを防ぐために、クライアントアクセスの特定の期間使用されていない既存のアクセスキャッシュエントリをクリアするための追加のパラメータがあります。これ `-harvest-timeout` パラメータの有効範囲は60~2、592、000秒で、デフォルト設定は86、400秒です。

qtree からエクスポートポリシーを削除する

qtree に割り当てられている特定のエクスポートポリシーが不要になった場合は、代わりに格納先ボリュームのエクスポートポリシーを継承するように qtree を変更することで、エクスポートポリシーを削除できます。これは、を使用して実行できます `volume qtree modify` コマンドにを指定します `-export-policy` パラメータと空の名前文字列（""）。

手順

1. qtree からエクスポートポリシーを削除するには、次のコマンドを入力します。

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy ""
   ```

2. qtree が適切に変更されたことを確認します。

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

qtree ファイル操作の **qtree ID** を検証します

ONTAP では、オプションで qtree ID の検証を追加で実行できます。この検証により、クライアントのファイル処理要求で有効な qtree ID が使用されるとともに、クライアントによるファイルの移動が同じ qtree 内でのみ行えるようになります。この検証を有効または無効にするには、を変更します `-validate-qtree-export` パラメータこのパラメータはデフォルトで有効になっています。

このタスクについて

このパラメータは、 Storage Virtual Machine （ SVM ）上の 1 つ以上の qtree にエクスポートポリシーを直接割り当てている場合にのみ有効です。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

検証する **qtree ID** の状態	入力するコマンド
有効	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`
無効	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

FlexVol のエクスポートポリシーの制限とネストされたジャンクション

上位レベルのジャンクションでネストされたジャンクションよりも制限が厳しいエクスポートポリシーを設定した場合は、下位レベルのジャンクションへのアクセスに失敗する可能性があります。

上位レベルのジャンクションには下位レベルのジャンクションよりも制限が厳しくないエクスポートポリシーを設定するようにしてください。

NFS で **Kerberos** を使用してセキュリティを強化する

ONTAP での **Kerberos** のサポート

Kerberos は、クライアント / サーバアプリケーションに対して強力でセキュアな認証を提供します。認証により、ユーザおよびプロセスの ID をサーバで検証できます。ONTAP 環境では、 Storage Virtual Machine （ SVM ）と NFS クライアント間の認証を Kerberos で実行できます。

ONTAP 9 では、次の Kerberos 機能がサポートされます。

- 整合性チェック機能を備えた Kerberos 5 認証（ krb5i ）

  Krb5i では、チェックサムを使用して、クライアントとサーバ間で転送される各 NFS メッセージの整合性を検証します。これは、セキュリティ上の理由（データが改ざんされていないことの確認など）とデータ整合性に関する理由（信頼性の低いネットワークで NFS を使用する場合のデータ破損の防止など）の両方で有用です。

- プライバシーチェック機能を備えた Kerberos 5 認証（ krb5p ）

  krb5p では、クライアントとサーバ間のすべてのトラフィックがチェックサムで暗号化されます。これにより、安全性が向上し、負荷も増加します。

- 128 ビットおよび 256 ビットの AES 暗号化

  Advanced Encryption Standard （ AES ）は、電子データを保護するための暗号化アルゴリズムです。ONTAPでは、セキュリティを強化するために、128ビットキーによるAES（AES-128）と256ビットキーによるAES（AES-256）がKerberosでサポートされます。

- SVM レベルの Kerberos Realm 設定

  SVM 管理者は、 Kerberos Realm 設定を SVM レベルで作成できるようになりました。つまり、 SVM 管理者は、 Kerberos Realm 設定に関してクラスタ管理者に頼る必要がなくなり、個別の Kerberos Realm 設定をマルチテナンシー環境で作成することができます。

NFS で **Kerberos** を設定するための要件

NFS で Kerberos を使用するための設定をシステムで行う前に、ネットワークおよびストレージの環境のいくつかの項目について、適切に設定されていることを確認する必要があります。

> 環境を設定する手順は、使用しているクライアントオペレーティングシステム、ドメインコントローラ、 Kerberos 、 DNS などのバージョンや種類によって異なります。これらのすべての変数については、本ドキュメントでは説明していません。詳細については、各コンポーネントの該当するドキュメントを参照してください。
>
> Windows Server 2008 R2 の Active Directory および Linux ホストを使用する環境での ONTAP と Kerberos 5 および NFSv3 / NFSv4 の設定方法に関する詳しい例については、テクニカルレポート 4073 を参照してください。

次の項目を最初に設定する必要があります。

ネットワーク環境の要件

- Kerberos

  Kerberos を Key Distribution Center （ KDC ；キー配布センター）で設定しておく必要があります（たとえば、 Windows Active Directory ベースの Kerberos または MIT Kerberos ）。

  NFSサーバはを使用する必要があります `nfs` マシンプリンシパルの主要コンポーネントとして使用します。

- ディレクトリサービス

  Active Directory や OpenLDAP などのセキュアなディレクトリサービスを環境に導入し、 SSL / TLS 経由の LDAP を使用するように設定する必要があります。

- NTP

  タイムサーバで NTP を実行している必要があります。これは、時刻のずれによる Kerberos 認証の失敗を

回避するために必要です。

- ドメイン名解決（ DNS ）

  それぞれの UNIX クライアントおよび SVM LIF について、 KDC の前方参照ゾーンと逆引き参照ゾーンに適切なサービスレコード（ SRV ）が登録されている必要があります。すべてのコンポーネントを DNS で正しく解決できる必要があります。

- ユーザアカウント

  各クライアントについて、 Kerberos Realm のユーザアカウントが必要です。NFS サーバでは ' マシン・プリンシパルの主要コンポーネントとして NFS' を使用する必要があります

NFSクライアントの要件

- NFS

  NFSv3 または NFSv4 を使用してネットワーク経由で通信するように各クライアントが適切に設定されている必要があります。

  クライアントで RFC1964 および RFC2203 がサポートされている必要があります。

- Kerberos

  Kerberos 認証を使用するように各クライアントが適切に設定されている必要があります。詳細は次のとおりです。

  - TGS 通信の暗号化が有効です。

    非常にセキュリティ性の高い AES-256 。

  - TGT 通信に対する最も安全な暗号化タイプが有効です。
  - Kerberos Realm とドメインを正しく設定します。
  - GSSはイネーブルです。

    マシンのクレデンシャルを使用する場合：

  - 走らないでください `gssd` を使用 `-n` パラメータ
  - 走らないでください `kinit` をrootユーザとして指定します。

- 各クライアントは、最新かつ更新されたオペレーティングシステムバージョンを使用する必要があります。

  これにより、 Kerberos での AES 暗号化の互換性と信頼性が最大限確保されます。

- DNS

  DNS を使用して名前が正しく解決されるように各クライアントが適切に設定されている必要があります。

- NTP

各クライアントが NTP サーバと同期されている必要があります。

- ホストおよびドメインの情報

  各クライアントの `/etc/hosts` および `/etc/resolv.conf` ファイルには正しいホスト名とDNS情報が格納されている必要があります。

- keytab ファイル

  各クライアントについて、 KDC の keytab ファイルが必要です。Realm は大文字で指定する必要があります。最高レベルのセキュリティを得るために、暗号化タイプを AES-256 にする必要があります。

- オプション：パフォーマンスを最大限に高めるには、ローカルエリアネットワークとの通信用とストレージネットワークとの通信用に、少なくとも 2 つのネットワークインターフェイスを設定します。

ストレージシステムの要件

- NFS ライセンス

  ストレージシステムに有効な NFS ライセンスがインストールされている必要があります。

- CIFSライセンス

  CIFS ライセンスはオプションです。マルチプロトコルのネームマッピングを使用する場合にのみ、Windows クレデンシャルをチェックする必要があります。純粋な UNIX のみの環境では必要ありません。

- SVM

  システムで SVM を少なくとも 1 つ設定しておく必要があります。

- SVM で DNS を設定します

  各 SVM で DNS を設定しておく必要があります。

- NFS サーバ

  SVM で NFS を設定しておく必要があります。

- AES 暗号化

  最高レベルのセキュリティを得るために、 Kerberos で AES-256 暗号化のみを許可するように NFS サーバを設定する必要があります。

- SMBサアハ

  マルチプロトコル環境の場合は、SVMでSMBを設定しておく必要があります。SMB サーバは、マルチプロトコルのネームマッピングに必要です。

- 個のボリューム

  SVM で使用するルートボリュームと少なくとも 1 つのデータボリュームを設定しておく必要があります。

- ルートボリューム

  SVM のルートボリュームを次のように設定しておく必要があります。

名前	設定
セキュリティ形式	「 UNIX 」
UID	root または ID 0
GID	root または ID 0
UNIX 権限	777

  ルートボリュームとは異なり、データボリュームのセキュリティ形式は任意に設定できます。

- UNIXグループ

  SVM で次の UNIX グループを設定しておく必要があります。

グループ名	グループ **ID**
デーモン	1.
ルート	0
pcuser	65534 （ SVM を作成すると ONTAP で自動的に作成されます）

- UNIXユーザ

  SVM で次の UNIX ユーザを設定しておく必要があります。

ユーザ名	ユーザ **ID**	プライマリグループ **ID**	コメント（ **Comment** ）
NFS	500ドル	0	GSS INITフェーズで必要 NFS クライアントユーザの SPN の最初のコンポーネントがユーザとして使用されます。

ユーザ名	ユーザ **ID**	プライマリグループ **ID**	コメント（ **Comment** ）
pcuser	65534	65534	NFSトCIFSノマルチフロトコルノシヨウニヒツヨウ SVMを作成すると、ONTAPで自動的に作成されてpcuserグループに追加されます。
ルート	0	0	マウントに必要

NFS クライアントユーザの SPN に対する Kerberos-UNIX ネームマッピングがある場合は、 nfs ユーザは必要ありません。

- エクスポートポリシーとルール

  ルートボリュームとデータボリュームおよび qtree に対するエクスポートポリシーと必要なエクスポートルールを設定しておく必要があります。SVMのすべてのボリュームへのアクセスにKerberosを使用する場合は、エクスポートルールのオプションを設定できます `-rorule`、 `-rwrule`および `-superuser` ルートボリュームのをに設定します `krb5` 、 `krb5i`または `krb5p`。

- Kerberos-UNIX ネームマッピング

  NFS クライアントユーザの SPN によって識別されたユーザに root 権限を持たせる場合は、 root に対するネームマッピングを作成する必要があります。

関連情報

"ネットアップテクニカルレポート 4073 ：『 Secure Unified Authentication 』"

"NetApp Interoperability Matrix Tool で確認できます"

"システム管理"

"論理ストレージ管理"

NFSv4 のユーザ **ID** ドメインを指定します

ユーザIDドメインを指定するには、を設定します `-v4-id-domain` オプション

このタスクについて

NFSv4 ユーザ ID のマッピングにデフォルトで使用されるドメインは、 NIS ドメインが設定されている場合は NIS ドメインになります。 ONTAPNIS ドメインが設定されていない場合は、 DNS ドメインが使用されます。たとえば、複数のユーザ ID ドメインがある場合、ユーザ ID ドメインの設定が必要になることがあります。ドメイン名は、ドメインコントローラのドメイン設定と一致する必要があります。これは NFSv3 の場合は必要ありません。

ステップ

1. 次のコマンドを入力します。

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

ネームサービスを設定

ONTAP のネームサービススイッチ設定の仕組み

ONTAP では、に相当するテーブルにネームサービス設定情報が格納されます `/etc/nsswitch.conf` UNIXシステム上のファイル。このテーブルを環境に応じて適切に設定するためには、その機能と ONTAP でテーブルがどのように使用されるかを理解しておく必要があります。

ONTAP ネームサービススイッチテーブルは、 ONTAP が特定の種類のネームサービス情報を取得する際にどのネームサービスソースをどの順番で参照するかを決定します。ONTAP では、 SVM ごとに個別のネームサービススイッチテーブルが保持されます。

データベースタイプ

テーブルには、次の各データベースタイプについてネームサービスのリストが格納されます。

データベースタイプ	ネームサービスソースの用途	有効なソース
ホスト	ホスト名の IP アドレスへの変換	ファイル、 DNS
グループ	ユーザグループ情報を検索しています	files 、 nis 、 ldap が表示されます
パスワード	ユーザ情報を検索しています	files 、 nis 、 ldap が表示されます
ネットグループ	ネットグループ情報の検索	files 、 nis 、 ldap が表示されます
namemap	ユーザ名のマッピング	ファイル、 LDAP

ソースタイプ

ソースタイプによって、該当する情報を取得するために使用するネームサービスソースが決まります。

ソースタイプ	情報の検索先	使用するコマンド

ファイル	ローカルのソースファイル	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

NIS	SVM の NIS ドメイン設定で指定された外部の NIS サーバ	`vserver services name-service nis-domain`
LDAP	SVM の LDAP クライアント設定で指定された外部の LDAP サーバ	`vserver services name-service ldap`
DNS	SVM の DNS 設定で指定された外部の DNS サーバ	`vserver services name-service dns`

データアクセスとSVM管理者の両方の認証にNISまたはLDAPを使用する場合も、を追加する必要があります `files` また、NISまたはLDAP認証が失敗した場合のフォールバックとしてローカルユーザを設定します。

外部ソースへのアクセスに使用するプロトコル

ONTAP では、外部ソースのサーバへのアクセスに次のプロトコルを使用します。

外部のネームサービスソース	アクセスに使用するプロトコル
NIS	UDP
DNS	UDP
LDAP	TCP

例

次の例では、 SVM svm_1 のネームサービススイッチ情報を表示しています。

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                 Source
Vserver         Database         Order
--------------- ------------     ---------
svm_1           hosts            files,
                                 dns
svm_1           group            files
svm_1           passwd           files
svm_1           netgroup         nis,
                                 files
```

ホストの IP アドレスの検索では、 ONTAP は最初にローカルのソースファイルを参照します。結果が返されない場合は、次に DNS サーバが照会されます。

ユーザまたはグループ情報の検索では、 ONTAP はローカルのソースファイルだけを参照します。結果が返されない場合、検索は失敗します。

ネットグループ情報の検索では、 ONTAP が最初に外部 NIS サーバを参照し、結果が返されない場合は、次にローカルネットグループファイルが照会されます。

SVM svm_1 のテーブルには、ネームマッピング用のネームサービスエントリは含まれていません。そのため、 ONTAP はデフォルトでローカルのソースファイルだけを参照します。

関連情報

"ネットアップテクニカルレポート 4668 ：『 Name Services Best Practices Guide 』"

LDAP を使用する

LDAPの概要

LDAP （ Lightweight Directory Access Protocol ）サーバを使用すると、ユーザ情報を一元的に管理できます。ユーザデータベースを LDAP サーバに保存する場合、既存の LDAP データベースのユーザ情報を検索するようにストレージシステムを設定できます。

- LDAP for ONTAP を設定する前に、サイト環境が LDAP サーバおよびクライアント設定のベストプラクティスを満たしていることを確認する必要があります。具体的には、次の条件を満たす必要があります。
  - LDAP サーバのドメイン名が LDAP クライアント上のエントリと一致している必要があります。
  - LDAP サーバでサポートされている LDAP ユーザパスワードハッシュタイプには、 ONTAP でサポートされているハッシュタイプが含まれている必要があります。
    - crypt （すべてのタイプ）および SHA-1 （ SHA 、 SSHA ）
    - ONTAP 9.8 以降では、 SHA-2 ハッシュ（ SHA-256 、 SSH-384 、 SHA-512 、 SSHA-256 、 SSHA-384 および SSHA-512 ）もサポートされます。
  - LDAP サーバにセッションセキュリティ対策が必要な場合は、 LDAP クライアントで設定する必要があります。

次のセッションセキュリティオプションを使用できます。

- LDAP 署名（データの整合性チェックを提供）および LDAP の署名と封印（データの整合性チェックと暗号化を提供）
- START TLS
- LDAPS （ LDAP over TLS または SSL ）

◦ 署名および封印された LDAP クエリを有効にするには、次のサービスが設定されている必要があります。

- LDAP サーバで GSSAPI （ Kerberos ） SASL がサポートされている必要があります。
- LDAP サーバに、 DNS A/AAAA レコード、および DNS サーバで設定された PTR レコードが必要です。
- Kerberos サーバに、 DNS サーバ上に存在する SRV レコードが必要です。

◦ TLS または LDAPS を開始できるようにするには、次の点を考慮する必要があります。

- ネットアップでは、 LDAPS ではなく Start TLS を使用することを推奨します。
- LDAPS を使用している場合は、 ONTAP 9.5 以降で LDAP サーバの TLS または SSL が有効になっている必要があります。ONTAP 9.0~9.4 では SSL はサポートされません。
- 証明書サーバがドメインで設定済みである必要があります。

◦ LDAP リファーラル追跡を有効にするには（ ONTAP 9.5 以降）、次の条件を満たしている必要があります。

- 両方のドメインで、次のいずれかの信頼関係を設定する必要があります。
  - 双方向
  - 一方向。一次は紹介ドメインを信頼します
  - 親子
- 参照されているすべてのサーバ名を解決するように DNS が設定されていること。
- の認証では、ドメインパスワードが同じである必要があります `--bind-as-cifs-server` trueに設定します。

> 次の設定は LDAP リファーラル追跡でサポートされません。
>
> ◦ すべての ONTAP バージョン：
>
> ◦ 管理 SVM 上の LDAP クライアント
>
> ◦ ONTAP 9.8 以前では（ 9.9.1 以降でサポートされています）：
>
> ◦ LDAPの署名と封印（ `-session-security` オプション）
>
> ◦ 暗号化されたTLS接続（ `-use-start-tls` オプション）
>
> ◦ LDAPSポート636（ `-use-ldaps-for-ad-ldap` オプション）

- ONTAP 9.11.1以降では、を使用できます "nsswitch認証のためのLDAP高速バインド。"
- SVM で LDAP クライアントを設定するときは、 LDAP スキーマを入力する必要があります。

  ほとんどの場合、デフォルトの ONTAP スキーマのいずれかが適しています。ただし、環境で使用する LDAP スキーマがこれらと異なる場合は、 LDAP クライアントを作成する前に、 ONTAP 用の新しい

LDAP クライアントスキーマを作成する必要があります。環境の要件については、 LDAP 管理者にお問い合わせください。

- LDAP をホスト名解決に使用することはサポートされていません。

追加情報の場合は、を参照してください "ネットアップテクニカルレポート 4835 ：『 How to Configure LDAP in ONTAP 』"。

LDAP の署名と封印の概念

ONTAP 9 以降では、署名と封印を設定して、 Active Directory （ AD ）サーバへの照会に対する LDAP セッションセキュリティを有効にすることができます。Storage Virtual Machine（SVM）のNFSサーバセキュリティ設定をLDAPサーバの設定に対応するように設定する必要があります。

署名は、シークレットキーのテクノロジを使用して、 LDAP ペイロードデータの整合性を確認します。封印は、 LDAP ペイロードデータを暗号化して機密情報がクリアテキストで送信されないようにします。LDAP トラフィックについて、署名が必要か、署名と封印が必要か、どちらも必要ないかは、 *ldap Security Level* オプションで指定します。デフォルトはです `none`。テスト

SMBトラフィックに対するLDAPの署名と封印は、を使用してSVMで有効にします `-session-security -for-ad-ldap` オプションをに設定します `vserver cifs security modify` コマンドを実行します

LDAPSの概念

ONTAP での LDAP 通信の保護方法に関する用語や概念を理解しておく必要があります。ONTAP は、 Active Directory 統合 LDAP サーバ間または UNIX ベース LDAP サーバ間の認証されたセッションの設定に Start TLS または LDAPS を使用できます。

用語集

ONTAP での LDAP 通信の保護に LDAPS を使用する方法に関して理解しておくべき用語があります。

- * LDAP *

  （ Lightweight Directory Access Protocol ）情報ディレクトリにアクセスして管理するためのプロトコルです。LDAP は、ユーザ、グループ、ネットグループなどのオブジェクトを格納するための情報ディレクトリとして使用されます。LDAP は、これらのオブジェクトを管理したり LDAP クライアントからの要求を満たしたりするディレクトリサービスも提供します。

- **SSL**

  （ Secure Sockets Layer ）インターネット上で情報を安全に送信するために開発されたプロトコルです。SSLはONTAP 9以降でサポートされていますが、TLSの導入に伴い廃止されました。

- * tls *

  （ Transport Layer Security ）従来の SSL 仕様に基づいた IETF 標準の追跡プロトコルです。SSL の後継にあたります。TLSはONTAP 9.5以降でサポートされます。

- * LDAPS （ LDAP over SSL または TLS ） *

TLS または SSL を使用して LDAP クライアントと LDAP サーバ間の通信を保護するプロトコル。「*ldap over SSL*」と「*ldap over TLS*」は同じ意味で使用されることがあります。LDAPSはONTAP 9.5以降でサポートされます。

- ONTAP 9.5-9.8 では、 LDAPS はポート 636 でのみ有効にできます。そのためには、を使用します `-use-ldaps-for-ad-ldap` パラメータと `vserver cifs security modify` コマンドを実行します
- ONTAP 9.9.1以降では、任意のポートでLDAPSを有効にできますが、デフォルトはポート636です。これを行うには、を設定します `-ldaps-enabled` パラメータの値 `true` そして目的のものを指定してください `-port` パラメータ詳細については、を参照してください `vserver services name-service ldap client create` のマニュアルページ

ネットアップでは、 LDAPS ではなく Start TLS を使用することを推奨します。

- * TLS を開始 *

  （ *START_TLS*,*STARTTLS* 、 *_StartTLS* とも呼ばれます）。 TLS プロトコルを使用してセキュアな通信を提供するメカニズムです。

  ONTAP では、 LDAP 通信を保護するために STARTTLS を使用し、デフォルトの LDAP ポート（ 389 ）を使用して LDAP サーバと通信します。LDAP サーバは、 LDAP ポート 389 経由の接続を許可するように設定する必要があります。そうしないと、 SVM から LDAP サーバへの LDAP TLS 接続が失敗します。

ONTAP での **LDAPS** の使用方法

ONTAP は TLS サーバ認証をサポートしています。この認証により、 SVM の LDAP クライアントは、バインド操作時に LDAP サーバの ID を確認できます。TLS に対応した LDAP クライアントは、公開鍵暗号化の標準的な技法を使用して、サーバの証明書および公開 ID が有効であり、かつクライアントの信頼できる Certificate Authority （ CA ；認証局）のリストにある CA によって発行されたものであるかどうかをチェックできます。

LDAP では、 TLS を使用した通信の暗号化方法として STARTTLS がサポートさSTARTTLS は標準の LDAP ポート（ 389 ）経由でプレーンテキスト接続として開始され、その後 TLS 接続にアップグレードされます。

ONTAP では次の機能がサポートされます

- Active Directory 統合 LDAP サーバと SVM の間の SMB 関連トラフィックに使用する LDAPS
- LDAPS ：ネームマッピングやその他の UNIX 情報で使用する LDAP トラフィックに使用します

  Active Directory 統合 LDAP サーバまたは UNIX ベース LDAP サーバのいずれかを使用して、 LDAP ネームマッピングおよびユーザ、グループ、ネットグループなどのその他の UNIX 情報の格納に使用できます。

- 自己署名ルート CA 証明書

  Active-Directory 統合 LDAP を使用している場合は、 Windows Server 証明書サービスがドメインにインストールされていると自己署名ルート証明書が生成されます。UNIX ベースの LDAP サーバを LDAP ネームマッピングに使用している場合は、該当する LDAP アプリケーションに適切な手段を使用して、自己署名ルート証明書の生成と保存が行われます。

デフォルトでは、LDAPSは無効になっています。

LDAP を使用するとともに、ネストされたグループメンバーシップを使用するための追加機能を必要とする場合は、 ONTAP を設定して LDAP の RFC2307bis サポートを有効にすることができます。

必要なもの

デフォルトの LDAP クライアントスキーマのうち、使用するいずれか 1 つのコピーを作成しておく必要があります。

このタスクについて

LDAP クライアントスキーマでは、グループオブジェクトによって memberUid 属性が使用されます。この属性には複数の値を含めることができ、そのグループに属するユーザの名前を一覧表示できます。RFC2307bis 対応の LDAP クライアントスキーマでは、グループオブジェクトによって uniqueMember 属性が使用されます。この属性には、 LDAP ディレクトリ内の別のオブジェクトの完全な Distinguished Name （ DN ；識別名）を含めることができます。これにより、グループに他のグループをメンバーとして追加できるため、ネストされたグループを使用できます。

このユーザは、ネストされたグループを含めて 256 を超えるグループのメンバーになることはできません。ONTAP は、この 256 グループの上限を超えるグループをすべて無視します。

デフォルトでは、 RFC2307bis サポートが無効になっています。

> MS-AD-BIS スキーマを使用して LDAP クライアントを作成すると、 ONTAP では RFC2307bis サポートが自動的に有効になります。

追加情報の場合は、を参照してください "ネットアップテクニカルレポート 4835 ：『 How to Configure LDAP in ONTAP 』"。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. コピーした RFC2307 LDAP クライアントスキーマを変更して、 RFC2307bis のサポートを有効にします。

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. LDAP サーバでサポートされているオブジェクトクラスに一致するように、スキーマを変更します。

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. LDAP サーバでサポートされている属性名に一致するように、スキーマを変更します。

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. admin 権限レベルに戻ります。

```
set -privilege admin
```

LDAP ディレクトリ検索の設定オプション

環境にとって最も適切な方法で LDAP サーバに接続するように ONTAP LDAP クライアントを設定することで、ユーザ、グループ、およびネットグループ情報を含め、 LDAP ディレクトリ検索を最適化することができます。デフォルトの LDAP ベースおよびスコープ検索値で十分な状況や、カスタム値のほうが適切な場合に指定すべきパラメータを理解しておく必要があります。

ユーザ、グループ、およびネットグループ情報の LDAP クライアント検索オプションは、 LDAP クエリの失敗、ひいてはストレージシステムへのクライアントアクセスの失敗を回避するのに役立ちます。また、クライアントのパフォーマンスの問題を回避するために、検索をできるだけ効率的に行うことができます。

デフォルトのベースおよびスコープ検索値です

LDAP ベースは、 LDAP クライアントが LDAP クエリを実行するために使用するデフォルトのベース DN です。ユーザ、グループ、ネットグループの検索を含むすべての検索は、ベース DN を使用して行われます。このオプションは、 LDAP ディレクトリが比較的小さく、すべての関連エントリが同じ DN 内にある場合に適しています。

カスタムベースDNを指定しない場合、デフォルトはです `root`。つまり、各クエリでディレクトリ全体が検索されます。これにより、 LDAP クエリが成功する見込みは最大になりますが、非効率的であったり、大規模な LDAP ディレクトリではパフォーマンスの大幅な低下につながったりする可能性があります。

LDAP ベーススコープは、 LDAP クライアントが LDAP クエリを実行するために使用するデフォルトの検索スコープです。ユーザ、グループ、ネットグループの検索を含むすべての検索は、ベーススコープを使用して行われます。LDAP クエリによる検索範囲を、名前付きエントリのみ、 DN の 1 レベル下にあるエントリ、または DN の下にあるサブツリー全体のどれにするかが決定されます。

カスタムベーススコープを指定しない場合、デフォルトはです `subtree`。つまり、各クエリで DN の下にあるサブツリー全体が検索されます。これにより、 LDAP クエリが成功する見込みは最大になりますが、非効率的であったり、大規模な LDAP ディレクトリではパフォーマンスの大幅な低下につながったりする可能性があります。

カスタムベースおよびスコープ検索値

必要に応じて、ユーザ、グループ、およびネットグループ検索で、別々のベースおよびスコープ値を指定できます。クエリの検索ベースとクエリをこうした形で制限すると、検索対象が LDAP ディレクトリのより小さなサブセクションに制限されるため、パフォーマンスを大幅に向上させることができます。

カスタムベースおよびスコープ値を指定した場合、ユーザ、グループ、およびネットグループ検索の一般的なデフォルト検索ベースおよびスコープは無視されます。カスタムベースおよびスコープ値を指定するパラメータは、 advanced 権限レベルで使用できます。

LDAP クライアントパラメータ	カスタム指定要素
`-base-dn`	すべての LDAP 検索のベース DN 複数の値を必要に応じて入力できます（ ONTAP 9.5 以降のリリースで LDAP リファーラル追跡を有効にした場合など）。

`-base-scope`	すべての LDAP 検索のベーススコープ
`-user-dn`	すべての LDAP ユーザ検索のベース DN このパラメータは、環境ユーザ名マッピング検索も行います。
`-user-scope`	すべての LDAP ユーザ検索のベーススコープ：このパラメータは、環境ユーザ名マッピング検索も行います。
`-group-dn`	すべての LDAP グループ検索のベース DN
`-group-scope`	すべての LDAP グループ検索のベーススコープ
`-netgroup-dn`	すべての LDAP ネットグループ検索のベース DN
`-netgroup-scope`	すべての LDAP ネットグループ検索のベーススコープ

複数のカスタムベース **DN** 値

LDAP ディレクトリが複雑な場合は、特定の情報を求めて LDAP ディレクトリの複数の部分を検索するために、複数のベース DN の指定が必要になることがあります。複数のユーザ、グループ、およびネットグループ DN パラメータを指定するには、各パラメータをセミコロン（ ; ）で区切り、 DN 検索リスト全体を二重引用符（ " ）で囲みます。DN にセミコロンが含まれている場合は、 DN のセミコロンの直前にエスケープ文字（ \ ）を追加する必要があります。

scope 環境は、対応するパラメータに指定されている のリスト全体を表します。たとえば、 3 つの異なるユーザ DN のリストとサブツリーをユーザスコープで指定した場合は、 LDAP ユーザ検索により、指定された 3 つの DN のそれぞれでサブツリー全体が検索されます。

また、 ONTAP 9.5 以降では、 LDAP_referral_c追いかけ _ を指定することもできます。これにより、プライマリ LDAP サーバから LDAP リファーラル応答が返されなかった場合に、 ONTAP LDAP クライアントがその他の LDAP サーバへのルックアップ要求を参照することができます。クライアントは、このリファーラルデータに記載されたサーバからターゲットオブジェクトを取得します。参照された LDAP サーバにあるオブジェクトを検索するには、参照されたオブジェクトのベース DN を LDAP クライアント設定の一部としてベース DN に追加します。ただし、参照されたオブジェクトは、（を使用して）リファーラル追跡が有効になっている場合にのみ検索されます `-referral-enabled true` オプション）LDAPクライアントの作成時または変更時

LDAP ディレクトリのホスト単位ネットグループ検索のパフォーマンスを向上させます

LDAP 環境がホスト単位のネットグループ検索を許可するように設定されている場合は、この機能を利用するように ONTAP を設定し、ホスト単位のネットグループ検索を実行することができます。これにより、ネットグループ検索の処理速度を大幅に引き上げ、ネットグループ検索時のレイテンシによる NFS クライアントアクセスの問題を減らすことができます。

必要なもの

LDAPディレクトリにはが含まれている必要があります `netgroup.byhost` 地図。

DNS サーバには、 NFS クライアントのフォワード（ A ）およびリバース（ PTR ）ルックアップレコードの両方が含まれている必要があります。

ネットグループ内の IPv6 アドレスを指定するときは、常に RFC 5952 で指定されているとおりに各アドレスを短縮および圧縮する必要があります。

このタスクについて

NISサーバは、と呼ばれる3つの個別のマップにネットグループ情報を格納します `netgroup`、`netgroup.byuser`および `netgroup.byhost`。の目的 `netgroup.byuser` および `netgroup.byhost` マップはネットグループ検索を高速化するためのものです。ONTAP は、マウントの応答時間を短縮するために NIS サーバ上でホスト単位のネットグループ検索を実行できます。

デフォルトでは、LDAPディレクトリにはそのようなはありません `netgroup.byhost` NISサーバと同様のマッピングただし、サードパーティのツールを使用すると、NISをインポートできます `netgroup.byhost` LDAPディレクトリにマッピングして、ホスト単位の高速ネットグループ検索を有効にします。ホスト単位のネットグループ検索を許可するようにLDAP環境を設定している場合は、を使用してONTAP LDAPクライアントを設定できます `netgroup.byhost` ホスト単位のネットグループ検索を高速化するために、名前、DN、および検索範囲をマッピングします。

ホスト単位のネットグループ検索の結果をより迅速に受け取ることで、 ONTAP クライアントがエクスポートへのアクセスを要求した場合、より高速にエクスポートルールを処理できます。これにより、ネットグループ検索による遅延の問題によってアクセスが遅延する可能性が低下します。

手順

1. NISの完全な識別名を取得します `netgroup.byhost` LDAPディレクトリにインポートしたマップ。

   マップ DN は、インポートに使用したサードパーティツールによって異なります。最高のパフォーマンスを得るには、正確なマップ DN を指定する必要があります。

2. 権限レベルを advanced に設定します。 `set -privilege advanced`
3. Storage Virtual Machine（SVM）のLDAPクライアント設定でホスト単位のネットグループ検索を有効にします。 `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost -dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled {true false}` LDAPディレクトリのホスト単位のネットグループ検索を有効または無効にします。デフォルトはです `false`。

   `-netgroup-byhost-dn netgroup-by-host_map_distinguished_name` の識別名を指定します `netgroup.byhost` LDAPディレクトリにマッピングします。これにより、ホスト単位のネットグループ検索のベース DN が無効になります。このパラメータを指定しない場合、 ONTAP は代わりにベース DN を使用します。

   `-netgroup-byhost-scope {base|onelevel subtree}` は、ホスト単位のネットグループ検索の検索範囲を指定します。このパラメータを指定しない場合、デフォルトのが使用されます `subtree`。

   LDAPクライアント設定がまだ存在しない場合は、を使用して新しいLDAPクライアント設定を作成するときにこれらのパラメータを指定することで、ホスト単位のネットグループ検索を有効にできます `vserver services name-service ldap client create` コマンドを実行します

ONTAP 9.2以降では、フィールドが表示されます `-ldap-servers` フィールドを置き換えます `-servers`。この新しいフィールドには、 LDAP サーバのホスト名または IP アドレスを指定できます。

4. admin 権限レベルに戻ります。 `set -privilege admin`

例

次のコマンドは、「ldap_corp」という名前の既存のLDAPクライアント設定を変更して、を使用したホスト単位のネットグループ検索を有効にします `netgroup.byhost` 「`nisMapName="netgroup.byhost"`、`dc=corp`、`dc=example`、`dc=com`」という名前のマップとデフォルトの検索範囲 `subtree`：

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

完了後

。 `netgroup.byhost` および `netgroup` クライアントアクセスの問題を回避するために、ディレクトリ内のマップは常に同期されている必要があります。

関連情報

"IETF RFC 5952 ：『 A Recommendation for IPv6 Address Text Representation 』"

nsswitch認証にLDAP高速バインドを使用できます

ONTAP 9.11.1以降では、ldap_fast bind_fルキノ ウ（_コンカレントbind_とも呼ばれます）を利用して、クライアント認証要求を迅速かつ簡単に行うことができます。この機能を使用するには、LDAPサーバが高速バインド機能をサポートしている必要があります。

このタスクについて

高速バインドを使用しない場合、ONTAP はLDAP簡易バインドを使用して、LDAPサーバで管理ユーザを認証します。この認証方式では、ONTAP がユーザまたはグループの名前をLDAPサーバに送信し、保存されているハッシュパスワードを受信して、サーバのハッシュコードをユーザパスワードからローカルに生成されたハッシュパスコードと比較します。同一の場合、ONTAP はログイン権限を付与します。

高速バインド機能を使用すると、ONTAP はセキュアな接続を介してLDAPサーバにユーザクレデンシャル（ユーザ名とパスワード）のみを送信します。LDAPサーバはこれらのクレデンシャルを検証し、ONTAP にログイン権限を付与するように指示します。

高速バインドの利点の1つは、LDAPサーバでサポートされるすべての新しいハッシュアルゴリズムをONTAPでサポートする必要がないことです。パスワードハッシュはLDAPサーバによって実行されるためです。

"高速バインドの使用方法について説明します。"

LDAP高速バインドには、既存のLDAPクライアント設定を使用できます。ただし、LDAPクライアントがTLSまたはLDAPS用に設定されていることを強く推奨します。設定されていない場合は、パスワードがプレーンテキストでネットワーク経由で送信されます。

ONTAP 環境でLDAP高速バインドを有効にするには、次の要件を満たす必要があります。

- ONTAP 管理者ユーザは、高速バインドをサポートするLDAPサーバで設定する必要があります。
- ネームサービススイッチ（nsswitch）データベースにLDAP用にONTAP SVMが設定されている必要があります。
- 高速バインドを使用してnsswitch認証を行うには、ONTAP 管理者ユーザアカウントとグループアカウントを設定する必要があります。

手順

1. LDAPサーバでLDAP高速バインドがサポートされていることをLDAP管理者に確認してください。
2. ONTAP 管理者ユーザクレデンシャルがLDAPサーバで設定されていることを確認します。
3. 管理SVMまたはデータSVMにLDAP高速バインドが正しく設定されていることを確認します。

   a. LDAP高速バインドサーバがLDAPクライアント設定にリストされていることを確認するには、次のように入力します。

      ```
      vserver services name-service ldap client show
      ```

      "LDAPクライアント設定について説明します。"

   b. 確認してください `ldap` は、nsswitchに設定されているソースの1つです `passwd` データベースに次のように入力します

      ```
      vserver services name-service ns-switch show
      ```

   "nsswitch設定の詳細は、こちらをご覧ください。"

4. 管理ユーザがnsswitchで認証されていること、およびアカウントでLDAP高速バインド認証が有効になっていることを確認します。

   - 既存のユーザの場合は、と入力します `security login modify` 次のパラメータ設定を確認します。

     ```
     -authentication-method nsswitch
     ```

   `-is-ldap-fastbind true`

   - 新しい管理者ユーザについては、を参照してください "LDAPまたはNISアカウントアクセスを有効にします。"

LDAP統計を表示します。

ONTAP 9.2 以降では、パフォーマンスを監視して問題を診断するために、ストレージシステム上の Storage Virtual Machine （ SVM ）の LDAP 統計を表示することができます。

必要なもの

- SVM で LDAP クライアントを設定しておく必要があります。
- データを表示できる LDAP オブジェクトを特定しておく必要があります。

ステップ

1. カウンタオブジェクトのパフォーマンスデータを表示します。

```
statistics show
```

例

次の例は、オブジェクトのパフォーマンスデータを表示します `secd_external_service_op`：

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance “vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1”

Object: secd_external_service_op
Instance: vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1
Start-time: 4/13/2016 22:15:38
End-time: 4/13/2016 22:15:38
Scope: vserverName
Counter                             Value
-------------------------------- --------------------------------
instance_name                       vserverName:LDAP (NIS & Name
                                    Mapping):GetUserInfoFromName:
                                    1.1.1.1
last_modified_time                  1460610787
node_name                           nodeName
num_not_found_responses             1
num_request_failures                1
num_requests_sent                   1
num_responses_received              1
num_successful_responses            0
num_timeouts                        0
operation                           GetUserInfoFromName
process_name                        secd
request_latency                     52131us
```

ネームマッピングを設定する

ネームマッピングの概要を設定する

ONTAPでは、ネームマッピングを使用して、SMB IDをUNIX IDに、Kerberos IDをUNIX IDに、UNIX IDをSMB IDにマッピングします。この情報は、NFSクライアントとSMBクライアントのどちらから接続しているかに関係なく、ユーザクレデンシャルを取得して適切なファイルアクセスを提供するために必要です。

ネームマッピングを使用する必要がない例外が 2 つあります。

- 純粋な UNIX 環境を構成しており、ボリュームに対して SMB アクセスや NTFS セキュリティ形式を使用する予定がない場合。
- 代わりにデフォルトユーザを使用するように設定している場合。

  このシナリオでは、すべてのクライアントクレデンシャルを個別にマッピングするのではなく、すべてのクライアントクレデンシャルが同じデフォルトユーザにマッピングされるため、ネームマッピングは必要ありません。

ネームマッピングはユーザに対してのみ使用でき、グループに対しては使用できません。

ただし、個々のユーザのグループを特定のユーザにマッピングすることはできます。たとえば、 SALES という単語が先頭または末尾に付くすべての AD ユーザを、特定の UNIX ユーザおよびそのユーザの UID にマッピングできます。

ネームマッピングの仕組み

ONTAP がユーザのクレデンシャルをマッピングする必要がある場合、最初に、ローカルのネームマッピングデータベースおよび LDAP サーバで既存のマッピングの有無をチェックします。一方をチェックするか両方をチェックするか、およびそのチェック順序は、 SVM のネームサービスの設定で決まります。

- Windows から UNIX へのマッピングの場合

  マッピングが見つからなかった場合、 ONTAP は小文字の Windows ユーザ名が UNIX ドメインで有効なユーザ名かどうかをチェックします。設定されている場合は、デフォルトの UNIX ユーザが使用されます。デフォルトの UNIX ユーザが設定されておらず、この方法でも ONTAP がマッピングを取得できない場合、マッピングは失敗し、エラーが返されます。

- UNIX から Windows へのマッピングの場合

  マッピングが見つからなかった場合、 ONTAP は SMB ドメインで UNIX 名と一致する Windows アカウントを探します。正しく設定されていない場合は、デフォルトの SMB ユーザが使用されます。デフォルトのSMBユーザが設定されておらず、この方法でもONTAPがマッピングを取得できない場合、マッピングは失敗し、エラーが返されます。

マシンアカウントは、デフォルトでは、指定したデフォルトの UNIX ユーザにマッピングされます。デフォルトの UNIX ユーザを指定しないと、マシンアカウントのマッピングは失敗します。

- ONTAP 9.5 以降では、マシンアカウントをデフォルトの UNIX ユーザ以外のユーザにマッピングできます。
- ONTAP 9.4 以前では、マシンアカウントを他のユーザにマッピングすることはできません。

  マシンアカウントに定義されているネームマッピングがあっても無視されます。

UNIX ユーザから **Windows** ユーザへのネームマッピングのためのマルチドメイン検索

ONTAP は、 UNIX ユーザを Windows ユーザにマッピングする際のマルチドメイン検索をサポートしています。一致する結果が返されるまで、検出されたすべての信頼できるドメインで、変換後のパターンに一致する名前が検索されます。また、信頼できる優先

ドメインのリストを設定することもできます。このリストは、検出された信頼できるドメインのリストの代わりに使用され、一致する結果が返されるまで順に検索されます。

ドメインの信頼性が **UNIX** ユーザから **Windows** ユーザへのネームマッピング検索に与える影響

マルチドメインのユーザ名マッピングの仕組みを理解するには、ドメインの信頼性が ONTAP に与える影響を理解しておく必要があります。SMBサーバのホームドメインとのActive Directory信頼関係は、双方向の信頼にすることも、インバウンドまたはアウトバウンドの2種類の単方向の信頼のいずれかにすることもできます。ホームドメインは、 SVM 上の SMB サーバが属しているドメインです。

- _ 双方向の信頼 _

  双方向の信頼では、両方のドメインが相互に信頼しています。SMBサーバのホームドメインが別のドメインと双方向の信頼関係にある場合、ホームドメインは信頼できるドメインに属するユーザを認証および許可できます。その逆も同様です。

  UNIX ユーザから Windows ユーザへのネームマッピング検索は、ホームドメインと他方のドメインの間に双方向の信頼関係が確立されたドメインでのみ実行できます。

- アウトバウンドの信頼 _

  アウトバウンドの信頼では、ホームドメインが他方のドメインを信頼しています。この場合、ホームドメインはアウトバウンドの信頼できるドメインに属しているユーザを認証および認可できます。

  ホームドメインとアウトバウンドの信頼関係にあるドメインは、 UNIX ユーザから Windows ユーザへのネームマッピング検索の実行時に _not_searched になります。

- インバウンドの信頼 _

  インバウンドの信頼では、もう一方のドメインがSMBサーバのホームドメインを信頼します。この場合、ホームドメインはインバウンドの信頼できるドメインに属しているユーザを認証または認可できません。

  ホームドメインとインバウンドの信頼関係にあるドメインは、 UNIX ユーザから Windows ユーザへのネームマッピング検索の実行時に _not_searched になります。

ワイルドカード（ * ）を使用したネームマッピングのためのマルチドメイン検索の設定

マルチドメインネームマッピング検索は、 Windows ユーザ名のドメインセクションにワイルドカードを使用することで容易になります。次の表に、マルチドメイン検索を有効にするためにネームマッピングエントリのドメイン部にワイルドカードを使用する方法を示します。

パターン（ **Pattern** ）	交換	結果
ルート	｛Asterisk｝　｛backslash｝　｛backslash｝　管理者	UNIX ユーザ「 root 」は「 administrator 」という名前のユーザにマッピングされます。「 administrator 」という名前の最初の一致するユーザが見つかるまで、すべての信頼できるドメインが順に検索されます。

パターン（ **Pattern** ）	交換	結果
*	｛Asterisk｝ ｛backslash｝ ｛backslash｝ ｛Asterisk｝	有効な UNIX ユーザは、対応する Windows ユーザにマッピングされます。該当する名前のユーザとの最初の一致が見つかるまで、すべての信頼できるドメインが順に検索されます。 ⓘ パターン ｛Asterisk｝ ｛backslash｝ ｛backslash｝ ｛Asterisk｝ は、UNIX から Windows へのネームマッピングでのみ有効で、反対方向では無効です。

マルチドメインの名前検索の実行方法

マルチドメインの名前検索に使用する信頼できるドメインのリストを決定する方法は 2 つあります。

- ONTAP で作成された自動検出された双方向の信頼リストを使用します
- 自分で作成した信頼できる優先ドメインリストを使用します

ユーザ名のドメインセクションにワイルドカードを使用して UNIX ユーザが Windows ユーザにマッピングされている場合、 Windows ユーザはすべての信頼できるドメインで次のように検索されます。

- 信頼できるドメインの優先リストが設定されている場合、マッピング先の Windows ユーザはこの検索リスト内でのみ順に検索されます。
- 信頼できるドメインの優先リストが設定されていない場合は、ホームドメインと双方向の信頼関係にあるすべてのドメインで Windows ユーザの検索が行われます。
- ホームドメインと双方向の信頼関係にあるドメインが存在しない場合、ホームドメインでユーザの検索が行われます。

UNIX ユーザがユーザ名にドメインセクションのない Windows ユーザにマッピングされている場合は、ホームドメインで Windows ユーザの検索が行われます。

ネームマッピングの変換ルール

ONTAP システムには、 SVM ごとに一連の変換ルールが保存されています。各ルールは、 a_pattern_ と a_replacement _ の 2 つの要素で構成されます。変換は該当するリストの先頭から開始され、最初に一致したルールに基づいて実行されます。パターンは UNIX 形式の正規表現です。リプレースメントは、UNIXのように、パターンのサブ式を表すエスケープシーケンスを含む文字列です `sed` プログラム。

ネームマッピングを作成します

を使用できます `vserver name-mapping create` コマンドを使用してネームマッピングを作成します。ネームマッピングを使用すると、 Windows ユーザから UNIX セキュリティ形式のボリュームへのアクセスおよびその逆方向のアクセスが可能になります。

このタスクについて

ONTAP では、 SVM ごとに、各方向について最大 12 、 500 個のネームマッピングがサポートされます。

ステップ

1. ネームマッピングを作成します。

   ```
   vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-
   unix|unix-win} -position integer -pattern text -replacement text
   ```

   > 。 `-pattern` および `-replacement` ステートメントは正規表現として記述できます。を使用することもできます `-replacement` null置換文字列を使用してユーザへのマッピングを明示的に拒否するステートメント `" "` （スペース文字）。を参照してください `vserver name-mapping create` のマニュアルページを参照してください。

   Windows から UNIX へのマッピングを作成した場合、新しいマッピングが作成されたときに ONTAP システムに接続していたすべての SMB クライアントは、新しいマッピングを使用するために、一度ログアウトしてから、再度ログインする必要があります。

例

次のコマンドは、 vs1 という名前の SVM 上にネームマッピングを作成します。このマッピングは UNIX から Windows へのマッピングで、優先順位リスト内での位置は 1 番目です。UNIX ユーザ johnd を Windows ユーザ ENG\JohnDoe にマッピングします。

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

次のコマンドは、 vs1 という名前の SVM 上に別のネームマッピングを作成します。このマッピングは Windows から UNIX へのマッピングで、優先順位リスト内での位置は 1 番目です。パターンとリプレースメントには正規表現が使用されています。このマッピングにより、ドメイン ENG 内のすべての CIFS ユーザが、 SVM に関連付けられた LDAP ドメイン内のユーザにマッピングされます。

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

次のコマンドは、 vs1 という名前の SVM 上に別のネームマッピングを作成します。このパターンには、エスケープする必要がある Windows ユーザ名の要素として「 $` 」が含まれています。Windows ユーザ ENG\john$ops を UNIX ユーザ john_ops にマッピングします。

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

デフォルトユーザを設定します。

ユーザに対する他のマッピングの試行がすべて失敗した場合や、 UNIX と Windows の間で個々のユーザをマッピングしないようにする場合に使用するデフォルトユーザを設定できます。ただし、マッピングされていないユーザの認証を失敗にする場合は、デフォルトユーザを設定しないでください。

このタスクについて

CIFS 認証で、各 Windows ユーザを個別の UNIX ユーザにマッピングしないようにする場合は、代わりにデフォルトの UNIX ユーザを指定できます。

NFS 認証で、各 UNIX ユーザを個別の Windows ユーザにマッピングしないようにする場合は、代わりにデフォルトの Windows ユーザを指定できます。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
デフォルトの UNIX ユーザを設定する	`vserver cifs options modify -default-unix-user user_name`
デフォルトの Windows ユーザを設定します	`vserver nfs modify -default-win-user user_name`

ネームマッピングの管理用コマンド

ONTAP には、ネームマッピングを管理するためのコマンドが用意されています。

状況	使用するコマンド
ネームマッピングを作成します	`vserver name-mapping create`
特定の位置にネームマッピングを挿入します	`vserver name-mapping insert`
ネームマッピングを表示します	`vserver name-mapping show`

2 つのネームマッピングの位置を入れ替えます 注：ネームマッピングにIP修飾子エントリが設定されている場合、スワップは許可されません。	`vserver name-mapping swap`
ネームマッピングを変更する	`vserver name-mapping modify`
ネームマッピングを削除する	`vserver name-mapping delete`
ネームマッピングが正しいことを確認します	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

詳細については、各コマンドのマニュアルページを参照してください。

Windows NFS クライアントのアクセスを有効にします

ONTAP は Windows NFSv3 クライアントからのファイルアクセスをサポートしています。つまり、NFSv3をサポートするWindowsオペレーティングシステムを実行しているクライアントは、クラスタのNFSv3エクスポートのファイルにアクセスできます。この機能を正しく使用するには、 Storage Virtual Machine （ SVM ）を適切に設定し、一定の要件と制限事項に注意する必要があります。

このタスクについて

デフォルトでは、 Windows NFSv3 クライアントサポートが無効になっています。

作業を開始する前に

SVM で NFSv3 が有効になっている必要があります。

手順

1. Windows NFSv3 クライアントのサポートを有効にします。

   ```
   vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly disabled
   ```

2. Windows NFSv3クライアントをサポートするすべてのSVMで、を無効にします `-enable-ejukebox` および `-v3-connection-drop` パラメータ：

   ```
   vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection-drop disabled
   ```

   これで、 Windows NFSv3 クライアントがストレージシステムにエクスポートをマウントできるようになります。

3. を指定して、各Windows NFSv3クライアントがハードマウントを使用するようにします `-o mtype=hard` オプション

これは、マウントの信頼性を確保するために必要です。

```
mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
```

NFS クライアントで NFS エクスポートの表示を有効にします

NFSクライアントはを使用できます `showmount -e` コマンドを使用して、ONTAP NFSサーバから使用可能なエクスポートのリストを表示します。これは、ユーザがマウントするファイルシステムを確認するのに役立ちます。

ONTAP 9.2 以降 ONTAP では、 NFS クライアントでのエクスポートリストの表示がデフォルトで許可されます。以前のリリースでは `showmount` のオプション `vserver nfs modify` コマンドは明示的に有効にする必要があります。エクスポートリストを表示するには、 SVM で NFSv3 が有効になっている必要があります。

例

次のコマンドは、 vs1 という SVM に対して showmount を実行します。

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1    enabled
```

次のコマンドは、 IP アドレスが 10.63.21.9 の NFS サーバ上のエクスポートのリストを表示します。

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix        (everyone)
/unix/unixl  (everyone)
/unix/unix2  (everyone)
/            (everyone)
```

NFSを使用したファイルアクセスの管理

NFSv3 を有効または無効にします

NFSv3を有効または無効にするには、を変更します `-v3` オプションこれにより、NFSv3プロトコルを使用してクライアントがファイルにアクセスできるようになります。デフォルトでは、 NFSv3 が有効になっています。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド

NFSv3 を有効にします	`vserver nfs modify -vserver vserver_name -v3 enabled`
NFSv3を無効にする	`vserver nfs modify -vserver vserver_name -v3 disabled`

NFSv4.0 を有効または無効にする

NFSv4.0を有効または無効にするには、 `-v4.0` オプションこれにより、 NFSv4.0 プロトコルを使用してクライアントがファイルにアクセスできるかどうかを指定できます。ONTAP 9.9.1では、NFSv4.0がデフォルトで有効になります。それより前のリリースでは、デフォルトで無効になっていました。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
NFSv4.0 を有効にする	`vserver nfs modify -vserver vserver_name -v4.0 enabled`
NFSv4.0 を無効にする	`vserver nfs modify -vserver vserver_name -v4.0 disabled`

NFSv4.1を有効または無効にする

NFSv4.1を有効または無効にするには、 `-v4.1` オプションこれにより、NFSv4.1プロトコルを使用してクライアントがファイルにアクセスできるようになります。ONTAP 9.9.1では、NFSv4.1がデフォルトで有効になります。以前のリリースでは、デフォルトで無効になっていました。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
NFSv4.1を有効にする	`vserver nfs modify -vserver vserver_name -v4.1 enabled`
NFSv4.1を無効にする	`vserver nfs modify -vserver vserver_name -v4.1 disabled`

NFSv4ストレージプールの制限を管理します

ONTAP 9.13以降では、クライアントあたりのストレージプールのリソース制限に達したときに、NFSv4サーバがNFSv4クライアントに対するリソースを拒否するように設定できます。クライアントがNFSv4ストレージプールリソースを大量に消費すると、NFSv4ストレージプールリソースが使用できないために他のNFSv4クライアントがブロックされる可能性があります。

この機能を有効にすると、各クライアントによるアクティブなストレージプールリソース消費量を表示することもできます。これにより、システムリソースを使い果たしているクライアントを識別しやすくなり、クライアントごとのリソース制限を課すことができます。

消費されたストレージプールリソースを表示します

。 `vserver nfs storepool show` コマンドは、消費されたストレージプールリソースの数を表示します。ストレージプールは、NFSv4クライアントが使用するリソースのプールです。

ステップ

1. 管理者としてを実行します `vserver nfs storepool show` コマンドを使用してNFSv4クライアントのstorepool情報を表示します。

例

次の例は、NFSv4クライアントのストレージプール情報を表示します。

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

-------------- --------- --------- ---------- ---------- ----------
---------

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

ストレージプール制限の制御を有効または無効にします

管理者は、次のコマンドを使用して、ストレージプールの制限制御を有効または無効にできます。

ステップ

1. 管理者は、次のいずれかの操作を実行します。

状況	入力するコマンド
ストレージプール制限の制御を有効にします	`vserver nfs storepool config modify -limit-enforce enabled`
ストレージプール制限の制御を無効にします	`vserver nfs storepool config modify -limit-enforce disabled`

ブロックされたクライアントのリストを表示します

ストレージプール制限が有効になっている場合、管理者は、クライアントごとのリソースしきい値に達したときにブロックされたクライアントを確認できます。管理者は次のコマンドを使用して、ブロックされたクライアントとしてマークされているクライアントを確認できます。

手順

1. を使用します `vserver nfs storepool blocked-client show` コマンドを使用してNFSv4ブロッククライアントリストを表示します。

ブロックされたクライアントリストからクライアントを削除します

クライアントあたりのしきい値に達したクライアントは切断され、ブロッククライアントキャッシュに追加されます。管理者は次のコマンドを使用して、ブロッククライアントキャッシュからクライアントを削除できます。これにより、クライアントはONTAP NFSv4サーバに接続できるようになります。

手順

1. を使用します `vserver nfs storepool blocked-client flush -client-ip <ip address>` コマンドを実行して、storepoolブロックされたクライアントキャッシュをフラッシュします。
2. を使用します `vserver nfs storepool blocked-client show` コマンドを使用して、クライアントがブロッククライアントキャッシュから削除されたことを確認します。

例

この例では、IPアドレスが「10.2.1.1」のブロックされたクライアントがすべてのノードからフラッシュされています。

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
----------
10.1.1.1

1 entries were displayed.
```

pNFS を有効または無効にします

pNFS は、 NFS クライアントがストレージデバイスに対する読み取り / 書き込み処理を直接かつ並行して実行し、ボトルネックとなる可能性がある NFS サーバをバイパスできるようにすることで、パフォーマンスを向上します。pNFS（Parallel NFS）を有効または無効にするには、を変更します `-v4.1-pnfs` オプション

ONTAP リリースの種類	pNFS のデフォルト値
9.8以降	無効
9.7以前	有効

必要なもの

pNFS を使用するには、 NFSv4.1 のサポートが必要です。

pNFS を有効にする場合は、まず NFS リファーラルを無効にする必要があります。両方を同時に有効にすることはできません。

SVM で pNFS と Kerberos を併用する場合は、 SVM 上のすべての LIF で Kerberos を有効にする必要があります。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
pNFS を有効にします	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`
pNFS を無効にします	`vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled`

関連情報

- NFSトランキングの概要

TCP および UDP 経由の NFS アクセスを制御します

TCPおよびUDP経由のStorage Virtual Machine（SVM）へのNFSアクセスを有効または無効にするには、を変更します `-tcp` および `-udp` パラメータを指定します。これにより、環境で NFS クライアントが TCP または UDP 経由でデータにアクセスできるかどうかを制御できます。

このタスクについて

これらのパラメータは NFS のみに適用されます。補助プロトコルには影響しません。たとえば、 TCP 経由の NFS が無効になっていても、 TCP 経由でのマウント処理は成功します。TCP または UDP トラフィックを完全にブロックするには、エクスポートポリシールールを使用します。

> コマンドの失敗を防ぐために、 NFS に対して TCP を無効にする前に SnapDiff RPC サーバをオフにする必要があります。TCPを無効にするには、コマンドを使用します `vserver snapdiff-rpc-server off -vserver vserver name`。

ステップ

1. 次のいずれかを実行します。

設定する NFS アクセスの状態	入力するコマンド
TCP 経由で有効化	`vserver nfs modify -vserver vserver_name -tcp enabled`
TCP 経由で無効化	`vserver nfs modify -vserver vserver_name -tcp disabled`
UDP経由で有効化	`vserver nfs modify -vserver vserver_name -udp enabled`
UDP 経由で無効にしました	`vserver nfs modify -vserver vserver_name -udp disabled`

非予約ポートからの NFS 要求を制御します

非予約ポートからのNFSマウント要求を拒否するには、を有効にします `-mount -rootonly` オプション非予約ポートからのすべてのNFS要求を拒否するには、を有効にします `-nfs-rootonly` オプション

このタスクについて

デフォルトでは、オプションです `-mount-rootonly` はです `enabled`。

デフォルトでは、オプションです `-nfs-rootonly` はです `disabled`。

これらのオプションは、 NULL 手順には適用されません。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
非予約ポートからの NFS マウント要求を許可します	`vserver nfs modify -vserver vserver_name -mount -rootonly disabled`
非予約ポートからの NFS マウント要求を拒否します	`vserver nfs modify -vserver vserver_name -mount -rootonly enabled`
非予約ポートからのすべての NFS 要求を許可します	`vserver nfs modify -vserver vserver_name -nfs -rootonly disabled`
非予約ポートからのすべての NFS 要求を拒否します	`vserver nfs modify -vserver vserver_name -nfs -rootonly enabled`

不明な **UNIX** ユーザ向けに、 **NTFS** ボリュームまたは **qtree** への **NFS** アクセスを処理する

ONTAP は、 NTFS セキュリティ形式のボリュームまたは qtree への接続を試みる UNIX ユーザを識別できない場合、そのユーザを Windows ユーザに明示的にマッピングできません。ONTAP は、セキュリティを厳しくするためにそのようなユーザに対してアクセスを拒否するように設定することも、そうしたユーザをデフォルトの Windows ユーザにマッピングしてすべてのユーザに最小限のレベルのアクセスを保証するように設定することもできます。

必要なもの

このオプションを有効にする場合は、デフォルトの Windows ユーザを設定する必要があります。

このタスクについて

UNIX ユーザが NTFS セキュリティ形式のボリュームまたは qtree へのアクセスを試みる場合、その UNIX ユーザは、 ONTAP が NTFS アクセス権を適切に評価できるように、まず Windows ユーザにマッピングされている必要があります。ただし、 ONTAP は、設定されているユーザ情報ネームサービスソースでその UNIX ユーザの名前を検索できなかった場合、特定の Windows ユーザにその UNIX ユーザを明示的にマッピングすることができません。このような不明な UNIX ユーザの処理方法は、次の方法で決定できます。

- 不明な UNIX ユーザに対してアクセスを拒否する。

  この場合、 NTFS ボリュームまたは qtree へのアクセス権を取得するためにすべての UNIX ユーザに明示的なマッピングを要求することで、より厳しいセキュリティが適用されます。

- 不明な UNIX ユーザをデフォルトの Windows ユーザにマッピングする。

  これにより、セキュリティは低下しますが、すべてのユーザがデフォルトの Windows ユーザを介して NTFS ボリュームまたは qtree への最小限のレベルのアクセス権を取得できるようになるため、利便性が向上します。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

不明な UNIX ユーザへのデフォルトの Windows ユーザのマッピング	入力するコマンド
有効	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled`
無効	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled`

3. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

非予約ポートを使用して **NFS** エクスポートをマウントするクライアントに関する注意事項

。 `-mount-rootonly` 非予約ポートを使用してNFSエクスポートをマウントするクライアントをサポートする必要があるストレージシステムでは、ユーザがrootとしてログインしている場合でも、オプションを無効にする必要があります。Hummingbird クライアントや Solaris NFS / IPv6 クライアントがこれに該当します。

状況に応じて `-mount-rootonly` オプションが有効になっている場合、ONTAP では、非予約ポート（1、023より大きいポート）を使用するNFSクライアントでNFSエクスポートをマウントすることはできません。

ドメインを検証してネットグループのより厳密なアクセスチェックを実行します

デフォルトでは、 ONTAP はネットグループに対するクライアントアクセスを評価する際に追加の検証を実行します。この追加チェックにより、クライアントのドメインが Storage Virtual Machine （ SVM ）のドメイン設定に一致していることが確認されます。一致しない場合、 ONTAP はクライアントアクセスを拒否します。

このタスクについて

ONTAP は、クライアントアクセス用のエクスポートポリシールールおよびネットグループが含まれているエクスポートポリシールールを評価する際に、クライアントの IP アドレスがそのネットグループに属しているかどうかを ONTAP が確認する必要があります。そのために、 ONTAP は、 DNS を使用してクライアントの IP アドレスをホスト名に変換し、 Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）を取得します。

ネットグループファイルにホストの短い名前のみがリストされていて、そのホストの短い名前が複数のドメインに存在している場合は、異なるドメインのクライアントがこのチェックなしでアクセス権を取得することが

可能です。

この問題を回避するために、 ONTAP は、ホストについて DNS から返されたドメインを SVM 用に設定されている DNS ドメイン名のリストと比較します。一致した場合は、アクセスが許可されます。一致しない場合、アクセスは拒否されます。

この検証はデフォルトで有効になっています。これを管理するには、を変更します `-netgroup-dns-domain-search` パラメータ。advanced権限レベルで使用できます。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 必要な操作を実行します。

ネットグループのドメイン検証の設定	入力するコマンド
有効	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain-search enabled`
無効	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain-search disabled`

3. 権限レベルを admin に設定します。

   ```
   set -privilege admin
   ```

NFSv3 サービスで使用されるポートを変更します

ストレージシステム上の NFS サーバは、マウントデーモンや Network Lock Manager などのサービスを使用して、特定のデフォルトネットワークポート経由で NFS クライアントと通信します。デフォルトポートは、ほとんどの NFS 環境で正しく機能するので変更する必要はありませんが、別の NFS ネットワークポートを NFSv3 環境で使用する場合はそうすることができます。

必要なもの

ストレージシステムで NFS ポートを変更するには、すべての NFS クライアントがシステムに再接続する必要があるため、変更に先立ってこの情報をユーザに伝えておく必要があります。

このタスクについて

NFS マウントデーモン、 Network Lock Manager （ NLM ；ネットワークロックマネージャ）、 Network Status Monitor （ NSM ；ネットワークステータスモニタ）、および NFS クォータデーモンの各サービスで使用されるポートを Storage Virtual Machine （ SVM ）ごとに設定できます。ポート番号の変更は、 TCP と UDP の両方でデータにアクセスする NFS クライアントに影響します。

NFSv4 および NFSv4.1 のポートは変更できません。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. NFS へのアクセスを無効にします。

   ```
   vserver nfs modify -vserver vserver_name -access false
   ```

3. 特定の NFS サービスの NFS ポートを設定します。

   ```
   vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
   ```

NFS ポートのパラメータ	説明	デフォルトのポート
`-mountd-port`	NFS マウントデーモン	635
`-nlm-port`	Network Lock Manager の略	4045
`-nsm-port`	Network Status Monitor サービスの略	4046
`-rquotad-port`	NFS クォータデーモン	4049

   デフォルトポートに加えて、 1 、 024~65 、 535 の範囲のポート番号を使用できます。各 NFS サービスは一意のポートを使用する必要があります。

4. NFS へのアクセスを有効にします。

   ```
   vserver nfs modify -vserver vserver_name -access true
   ```

5. を使用します `network connections listening show` ポート番号の変更を確認するコマンド。
6. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

例

次のコマンドは、 vs1 という SVM で NFS マウントデーモンのポートを 1113 に設定します。

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- --------------------------------  ----------------
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700          TCP/ctlopcp
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:1113                       TCP/mount
vs1              data1:1113                       UDP/mount
...
vs1::*> set -privilege admin
```

NFS サーバを管理するためのコマンドです

ONTAP には、 NFS サーバを管理するためのコマンドが用意されています。

状況	使用するコマンド
NFS サーバを作成します	`vserver nfs create`
NFS サーバを表示する	`vserver nfs show`
NFS サーバを変更する	`vserver nfs modify`
NFS サーバを削除する	`vserver nfs delete`

を非表示にします `.snapshot` NFSv3マウントポイント下のディレクトリリスト への明示的なアクセス `.snapshot` このオプションが有効になっていても、ディレクトリは許可されます。	`vserver nfs` を使用したコマンド `-v3-hide-snapshot` オプションを有効にします

詳細については、各コマンドのマニュアルページを参照してください。

ネームサービスの問題をトラブルシューティングする

ネームサービスの問題でクライアントでアクセスエラーが発生した場合は、を使用できます `vserver services name-service getxxbyyy` さまざまなネームサービス検索を手動で実行し、検索の詳細と結果を調べてトラブルシューティングに役立てるためのコマンドファミリー。

このタスクについて

- 各コマンドでは、次の情報を指定できます。
  - 検索を実行するノードまたは Storage Virtual Machine （ SVM ）の名前。

    これにより、特定のノードまたは SVM でネームサービス検索をテストして、想定されるネームサービス設定問題の検索を絞り込むことができます。

  - 検索に使用されるソースを表示するかどうか。

    これにより、正しいソースが使用されているかどうかを確認できます。

- ONTAP は、設定されているネームサービススイッチの順序に基づいて、検索を実行するためのサービスを選択します。
- これらのコマンドは advanced 権限レベルで使用できます。

手順

1. 次のいずれかを実行します。

取得する情報	使用するコマンド
ホスト名のIPアドレス	`vserver services name-service getxxbyyy getaddrinfo` `vserver services name-service getxxbyyy gethostbyname` （IPv4アドレスのみ）
グループIDごとのグループのメンバー	`vserver services name-service getxxbyyy getgrbygid`

グループ名ごとのグループのメンバー	`vserver services name-service getxxbyyy getgrbyname`
ユーザが属しているグループのリスト	`vserver services name-service getxxbyyy getgrlist`
IPアドレスのホスト名	`vserver services name-service getxxbyyy getnameinfo` `vserver services name-service getxxbyyy gethostbyaddr` （IPv4アドレスのみ）
ユーザ名別のユーザ情報	`vserver services name-service getxxbyyy getpwbyname` RBACユーザの名前解決をテストするには、を指定します `-use-rbac` パラメータの形式 `true`。
ユーザIDごとのユーザ情報	`vserver services name-service getxxbyyy getpwbyuid` RBACユーザの名前解決をテストするには、を指定します `-use-rbac` パラメータの形式 `true`。
クライアントのネットグループメンバーシップ	`vserver services name-service getxxbyyy netgrp`
ホスト単位のネットグループ検索を使用したクライアントのネットグループメンバーシップ	`vserver services name-service getxxbyyy netgrpbyhost`

次の例は、ホストacast1.eng.example.comのIPアドレスの取得を試みることでSVM vs1のDNSルックアップをテストします。

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

次の例は、501768というUIDを持つユーザのユーザ情報の取得を試みることでSVM vs1のNIS検索をテストします。

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

次の例は、ldap1というユーザのユーザ情報の取得を試みることでSVM vs1のLDAP検索をテストします。

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

次の例は、クライアントdnshost0がネットグループlnetgroup136のメンバーであるかどうかを調べることでSVM vs1のネットグループ検索をテストします。

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. 実行したテストの結果を分析し、必要な措置を取ります。

状況	を確認します
ホスト名または IP アドレスの検索に失敗したか、正しくない結果が得られました	DNS設定
検索で間違ったソースが照会されました	ネームサービススイッチの設定

状況	を確認します
ユーザまたはグループの検索に失敗したか、正しくない結果が得られた	• ネームサービススイッチの設定 • ソースの設定（ローカルファイル、NISドメイン、LDAPクライアント） • ネットワーク設定（ LIF 、ルートなど）
ホスト名の検索に失敗したかタイムアウトになり、DNS の短縮名（例： host1 ）が DNS サーバで解決されない	Top-Level Domain（TLD；最上位レベルのドメイン）クエリのDNS設定。を使用して、TLDクエリを無効にできます `-is-tld-query-enabled false` オプションをに設定します `vserver services name-service dns modify` コマンドを実行します

関連情報

"ネットアップテクニカルレポート 4668 ：『 Name Services Best Practices Guide 』"

ネームサービスの接続を確認

ONTAP 9.2 以降では、 DNS ネームサーバと LDAP ネームサーバが ONTAP に接続されているかどうかを確認できます。これらのコマンドは admin 権限レベルで使用できます。

このタスクについて

DNS または LDAP ネームサービスの設定が有効かどうかは、必要に応じてネームサービス設定チェックを使用して確認できます。この検証チェックは、コマンドラインまたは System Manager で実行できます。

DNS 設定の場合、すべてのサーバがテストされ、設定が有効とみなされるためにはすべてのサーバが動作している必要があります。LDAP 設定の場合は、いずれかのサーバが稼働していれば設定は有効です。ネームサービスコマンドでは、以外の設定チェックが適用されます `skip-config-validation` フィールドはtrue（デフォルトはfalse）です。

ステップ

1. 適切なコマンドを使用して、ネームサービスの設定を確認します。設定されているサーバのステータスが UI に表示されます。

確認する項目	使用するコマンド
DNS の設定ステータス	`vserver services name-service dns check`
LDAPの設定ステータス	`vserver services name-service ldap check`

```
cluster1::> vserver services name-service dns check -vserver vs0

Vserver         Name Server     Status  Status Details
--------------  --------------- ------- -------------------------
 vs0            10.11.12.13     up      Response time (msec): 55
 vs0            10.11.12.14     up      Response time (msec): 70
 vs0            10.11.12.15     down    Connection refused.
+-------------------------------------------------------------+
```

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                |
| Client Configuration Name: c1                               |
| LDAP Status: up                                             |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                              |
```

設定されているサーバ（ name-servers/ldap-servers ）の少なくとも 1 つが到達可能でサービスを提供していれば、設定の検証は成功です。到達不能なサーバがある場合は、警告が表示されます。

ネームサービススイッチエントリを管理するコマンド

ネームサービススイッチエントリは、作成、表示、変更、および削除することで管理できます。

状況	使用するコマンド
ネームサービススイッチエントリを作成します	`vserver services name-service ns-switch create`
ネームサービススイッチエントリを表示します	`vserver services name-service ns-switch show`
ネームサービススイッチエントリを変更する	`vserver services name-service ns-switch modify`
ネームサービススイッチエントリを削除する	`vserver services name-service ns-switch delete`

詳細については、各コマンドのマニュアルページを参照してください。

関連情報

"ネットアップテクニカルレポート 4668 ：『 Name Services Best Practices Guide 』"

ネームサービスキャッシュを管理するコマンド

ネームサービスキャッシュは、 Time-To-Live （ TTL ）値を変更することで管理できます。TTL 値は、ネームサービス情報がキャッシュに保持される期間です。

TTL 値を変更する対象	使用するコマンド
UNIX ユーザ	`vserver services name-service cache unix-user settings`
UNIX グループ	`vserver services name-service cache unix-group settings`
UNIX ネットグループ	`vserver services name-service cache netgroups settings`
ホスト	`vserver services name-service cache hosts settings`
グループメンバーシップ	`vserver services name-service cache group-membership settings`

関連情報

"ONTAP 9コマンド"

ネームマッピングの管理用コマンド

ONTAP には、ネームマッピングを管理するためのコマンドが用意されています。

状況	使用するコマンド
ネームマッピングを作成します	`vserver name-mapping create`
特定の位置にネームマッピングを挿入します	`vserver name-mapping insert`
ネームマッピングを表示します	`vserver name-mapping show`
2 つのネームマッピングの位置を入れ替えます 注：ネームマッピングにIP修飾子エントリが設定されている場合、スワップは許可されません。	`vserver name-mapping swap`
ネームマッピングを変更する	`vserver name-mapping modify`

ネームマッピングを削除する	`vserver name-mapping delete`
ネームマッピングが正しいことを確認します	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

詳細については、各コマンドのマニュアルページを参照してください。

ローカル **UNIX** ユーザを管理するためのコマンド

ONTAP には、ローカル UNIX ユーザを管理するための固有のコマンドが用意されています。

状況	使用するコマンド
ローカル UNIX ユーザを作成します	`vserver services name-service unix-user create`
URI からローカル UNIX ユーザをロードします	`vserver services name-service unix-user load-from-uri`
ローカル UNIX ユーザを表示します	`vserver services name-service unix-user show`
ローカル UNIX ユーザを変更する	`vserver services name-service unix-user modify`
ローカル UNIX ユーザを削除する	`vserver services name-service unix-user delete`

詳細については、各コマンドのマニュアルページを参照してください。

ローカル **UNIX** グループを管理するためのコマンド

ONTAP には、ローカル UNIX グループを管理するための固有のコマンドが用意されています。

状況	使用するコマンド
ローカル UNIX グループを作成します	`vserver services name-service unix-group create`
ローカル UNIX グループにユーザを追加します	`vserver services name-service unix-group adduser`
URI からローカル UNIX グループをロードします	`vserver services name-service unix-group load-from-uri`

ローカル UNIX グループを表示します	`vserver services name-service unix-group show`
ローカル UNIX グループを変更する	`vserver services name-service unix-group modify`
ローカル UNIX グループからユーザを削除します	`vserver services name-service unix-group deluser`
ローカル UNIX グループを削除する	`vserver services name-service unix-group delete`

詳細については、各コマンドのマニュアルページを参照してください。

ローカル **UNIX** ユーザ、グループ、およびグループメンバーに対する制限

ONTAP では、クラスタ内の UNIX ユーザおよびグループの最大数の制限と、この制限を管理するためのコマンドが導入されました。これらの制限は、管理者がクラスタ内にローカル UNIX ユーザおよびグループを過剰に作成できないようにすることで、パフォーマンスの問題を回避するのに役立ちます。

ローカル UNIX ユーザグループとグループメンバーの合計数には制限があります。ローカル UNIX ユーザについては別途制限があります。これらの制限はクラスタ全体に適用されます。これらの新しい制限はそれぞれデフォルト値に設定されており、あらかじめ割り当てられたハードリミットまで引き上げることができます。

データベース	デフォルトの制限です	ハードリミット
ローカル UNIX ユーザ	３２、７６８	六五、五三六
ローカル UNIX グループおよびグループメンバー	３２、７６８	六五、五三六

ローカル **UNIX** ユーザおよびグループの制限を管理します

ONTAP には、ローカル UNIX ユーザおよびグループに対する制限を管理するための固有のコマンドが用意されています。クラスタ管理者は、これらのコマンドを使用して、過剰な数のローカル UNIX ユーザおよびグループに関連していると考えられる、クラスタ内のパフォーマンスの問題のトラブルシューティングを行うことができます。

このタスクについて

これらのコマンドは、 advanced 権限レベルのクラスタ管理者が使用できます。

ステップ

1. 次のいずれかを実行します。

状況	使用するコマンド
ローカル UNIX ユーザの制限に関する情報を表示する	`vserver services unix-user max-limit show`
ローカル UNIX グループの制限に関する情報を表示します	`vserver services unix-group max-limit show`
ローカル UNIX ユーザの制限を変更する	`vserver services unix-user max-limit modify`
ローカル UNIX グループの制限を変更する	`vserver services unix-group max-limit modify`

詳細については、各コマンドのマニュアルページを参照してください。

ローカルネットグループの管理用コマンド

URI からのロード、ノード間でのステータスの確認、表示、削除を行うことで、ローカルネットグループを管理できます。

状況	使用するコマンド
URI からネットグループをロードします	`vserver services name-service netgroup load`
ノード間でのネットグループのステータスを確認します	`vserver services name-service netgroup status` advanced 権限レベル以上で使用できます。
ローカルネットグループを表示します	`vserver services name-service netgroup file show`
ローカルネットグループを削除する	`vserver services name-service netgroup file delete`

詳細については、各コマンドのマニュアルページを参照してください。

NIS ドメイン設定を管理するコマンドです

ONTAP には、 NIS ドメイン設定を管理するためのコマンドが用意されています。

状況	使用するコマンド
NIS ドメイン設定を作成します	`vserver services name-service nis-domain create`

NISドメイン設定を表示する	`vserver services name-service nis-domain show`
NIS ドメイン設定のバインドステータスを表示します	`vserver services name-service nis-domain show-bound`
NIS統計を表示する	`vserver services name-service nis-domain show-statistics` advanced 権限レベル以上で使用できます。
NIS の統計を消去します	`vserver services name-service nis-domain clear-statistics` advanced 権限レベル以上で使用できます。
NIS ドメイン設定を変更する	`vserver services name-service nis-domain modify`
NIS ドメイン設定を削除する	`vserver services name-service nis-domain delete`
ホスト単位のネットグループ検索でのキャッシュを有効にします	`vserver services name-service nis-domain netgroup-database config modify` advanced 権限レベル以上で使用できます。

詳細については、各コマンドのマニュアルページを参照してください。

LDAP クライアント設定の管理用コマンド

ONTAP には、 LDAP クライアント設定を管理するためのコマンドが用意されています。

> SVM 管理者は、クラスタ管理者が作成した LDAP クライアント設定を変更したり削除したりできません。

状況	使用するコマンド
LDAP クライアント設定を作成します	`vserver services name-service ldap client create`
LDAP クライアント設定を表示します	`vserver services name-service ldap client show`
LDAP クライアント設定を変更します	`vserver services name-service ldap client modify`
LDAP クライアントのバインドパスワードを変更します	`vserver services name-service ldap client modify-bind-password`
LDAP クライアント設定を削除します	`vserver services name-service ldap client delete`

詳細については、各コマンドのマニュアルページを参照してください。

LDAP 設定を管理するためのコマンド

ONTAP には、 LDAP 設定を管理するためのコマンドが用意されています。

状況	使用するコマンド
LDAP 設定を作成します	`vserver services name-service ldap create`
LDAP 設定を表示します	`vserver services name-service ldap show`
LDAP 設定を変更します	`vserver services name-service ldap modify`
LDAP 設定を削除します	`vserver services name-service ldap delete`

詳細については、各コマンドのマニュアルページを参照してください。

LDAP クライアントスキーマテンプレートを管理するためのコマンド

ONTAP には、 LDAP クライアントスキーマテンプレートを管理するための固有のコマンドが用意されています。

SVM 管理者は、クラスタ管理者が作成した LDAP クライアントスキーマを変更したり削除したりできません。

状況	使用するコマンド
既存の LDAP スキーマテンプレートをコピーします	`vserver services name-service ldap client schema copy` advanced 権限レベル以上で使用できます。
LDAP スキーマテンプレートを表示します	`vserver services name-service ldap client schema show`
LDAP スキーマテンプレートを変更します	`vserver services name-service ldap client schema modify` advanced 権限レベル以上で使用できます。
LDAP スキーマテンプレートを削除します	`vserver services name-service ldap client schema delete` advanced 権限レベル以上で使用できます。

詳細については、各コマンドのマニュアルページを参照してください。

NFS Kerberos インターフェイス設定を管理するコマンドです

ONTAP には、 NFS Kerberos インターフェイスの設定を管理するためのコマンドが用意

されています。

状況	使用するコマンド
LIF で NFS Kerberos を有効にします	`vserver nfs kerberos interface enable`
NFS Kerberos インターフェイスの設定を表示します	`vserver nfs kerberos interface show`
NFS Kerberos インターフェイスの設定を変更します	`vserver nfs kerberos interface modify`
LIF で NFS Kerberos を無効にします	`vserver nfs kerberos interface disable`

詳細については、各コマンドのマニュアルページを参照してください。

NFS Kerberos Realm 設定を管理するコマンド

ONTAP には、 NFS Kerberos Realm の設定を管理するための固有のコマンドが用意されています。

状況	使用するコマンド
NFS Kerberos Realm の設定を作成します	`vserver nfs kerberos realm create`
NFS Kerberos Realm の設定を表示します	`vserver nfs kerberos realm show`
NFS Kerberos Realm の設定を変更します	`vserver nfs kerberos realm modify`
NFS Kerberos Realm の設定を削除します	`vserver nfs kerberos realm delete`

詳細については、各コマンドのマニュアルページを参照してください。

エクスポートポリシーを管理するためのコマンド

ONTAP には、エクスポートポリシーを管理するためのコマンドが用意されています。

状況	使用するコマンド
エクスポートポリシーに関する情報を表示します	`vserver export-policy show`

エクスポートポリシーの名前を変更します	`vserver export-policy rename`
エクスポートポリシーをコピーする	`vserver export-policy copy`
エクスポートポリシーを削除する	`vserver export-policy delete`

詳細については、各コマンドのマニュアルページを参照してください。

エクスポートルールを管理するためのコマンド

ONTAP には、エクスポートルールを管理するためのコマンドが用意されています。

状況	使用するコマンド
エクスポートルールを作成します	`vserver export-policy rule create`
エクスポートルールに関する情報を表示する	`vserver export-policy rule show`
エクスポートルールを変更する	`vserver export-policy rule modify`
エクスポートルールを削除する	`vserver export-policy rule delete`

> 異なるクライアントを照合する同一のエクスポートルールが複数設定されている場合は、エクスポートルールの管理時にそれらのルールの同期を必ず維持するようにしてください。

詳細については、各コマンドのマニュアルページを参照してください。

NFS クレデンシャルキャッシュを設定する

NFS クレデンシャルキャッシュの Time-To-Live を変更する理由

ONTAP は、アクセス高速化とパフォーマンス向上のために、クレデンシャルキャッシュを使用して、 NFS エクスポートアクセスでのユーザ認証に必要な情報を格納します。情報がクレデンシャルキャッシュに格納される期間を設定して、環境に合わせてカスタマイズできます。

NFS クレデンシャルキャッシュの Time-To-Live （ TTL ）の変更が問題の解決に役立つ場合があります。どのような状況がこれに該当するか、またそうした変更がどのような影響を及ぼすかを理解しておく必要があります。

理由

次の状況では、デフォルト TTL の変更を検討してください。

問題	修正アクション
環境内のネームサーバで ONTAP からの要求の負荷が高いためにパフォーマンスが低下している。	キャッシュされている受理および拒否のクレデンシャルに対する TTL を長くして、 ONTAP からネームサーバへの要求数を減らします。
ネームサーバ管理者がこれまで拒否されていた NFS ユーザに対してアクセスを許可する変更を行った。	キャッシュされている拒否されたクレデンシャルに対する TTL を短くして、 ONTAP ユーザが新しいクレデンシャルを外部ネームサーバに要求して NFS ユーザがアクセスできるようになるまでの待機時間を短縮します。
ネームサーバ管理者がこれまで許可されていた NFS ユーザに対してアクセスを拒否する変更を行った。	キャッシュされている受理されたクレデンシャルに対する TTL を短くして、 ONTAP が新しいクレデンシャルを外部ネームサーバに要求して NFS ユーザがアクセスを拒否されるようになるまでの時間を短縮します。

結果

受理および拒否のクレデンシャルをキャッシュしておく期間を個別に変更することができます。ただし、こうした変更の長所と短所の両方に注意する必要があります。

状況	利点は ...	欠点は ...
クレデンシャルのキャッシュ時間を長くしてください	ONTAP がクレデンシャルの要求をネームサーバに送信する頻度が低下し、ネームサーバの負荷が軽減されます。	それまではアクセスが許可されていたが今後は許可されなくなる NFS ユーザに対し、アクセスを拒否するのにかかる時間が長くなります。
受理されたクレデンシャルのキャッシュ時間を短くします	それまではアクセスが許可されていたが今後は許可されなくなる NFS ユーザに対し、アクセスを拒否するのにかかる時間が短くなります。	ONTAP がクレデンシャルの要求をネームサーバに送信する頻度が高くなり、ネームサーバの負荷が増大します。
拒否されたクレデンシャルのキャッシュ時間を長くします	ONTAP がクレデンシャルの要求をネームサーバに送信する頻度が低下し、ネームサーバの負荷が軽減されます。	それまではアクセスが許可されていなかったが今後は許可されるようになる NFS ユーザに対し、アクセスを許可するのにかかる時間が長くなります。
拒否されたクレデンシャルのキャッシュ時間を短くします	それまではアクセスが許可されていなかったが今後は許可されるようになる NFS ユーザに対し、アクセスを許可するのにかかる時間が短くなります。	ONTAP がクレデンシャルの要求をネームサーバに送信する頻度が高くなり、ネームサーバの負荷が増大します。

キャッシュされた **NFS** ユーザクレデンシャルの **Time-To-Live** を設定してください

Storage Virtual Machine （ SVM ）の NFS サーバを変更することで、 ONTAP が NFS ユーザのクレデンシャルを内部キャッシュに格納する期間である Time-To-Live （ TTL ）を設定できます。これにより、ネームサーバの高負荷に関する問題や、 NFS ユーザアクセスに影響を及ぼすクレデンシャルの変更に関する問題を軽減できます。

このタスクについて

これらのパラメータは advanced 権限レベルで使用できます。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 必要な操作を実行します。

TTL を変更するキャッシュ対象	使用するコマンド
受理のクレデンシャル	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` TTL の測定単位はミリ秒です。ONTAP 9.10.1以降では、デフォルトは1時間（3,600,000ミリ秒）です。 ONTAP 9.9.1以前では、デフォルトは24時間（86、400,000ミリ秒）です。 この値の許容範囲は 1 分（ 60 、 000 ミリ秒） ~7 日間（ 604 、 800 、 000 ミリ秒）です。
拒否のクレデンシャルです	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` TTL の測定単位はミリ秒です。デフォルトは 2 時間（ 7,200,000 ミリ秒）です。この値の許容範囲は 1 分（ 60 、 000 ミリ秒） ~7 日間（ 604 、 800 、 000 ミリ秒）です。

3. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

エクスポートポリシーキャッシュを管理します

エクスポートポリシーキャッシュをフラッシュします

ONTAP は、アクセスを高速化するために、エクスポートポリシーに関連する情報の格納に複数のエクスポートポリシーキャッシュを使用します。エクスポートポリシーキャッシュを手動でフラッシュします (`vserver export-policy cache flush`)古い可能性がある情報を削除し、ONTAP が適切な外部リソースから最新情報を取得するように強制します。これは、 NFS エクスポートへのクライアントアクセスに関するさまざまな問

題の解決に役立ちます。

このタスクについて

エクスポートポリシーキャッシュの情報は、次の理由で古くなる可能性があります。

- エクスポートポリシールールが最近変更された
- ネームサーバでホスト名レコードが最近変更された
- ネームサーバでネットグループエントリが最近変更された
- ネットグループの完全なロードを妨げていたネットワーク停止からのリカバリが発生しました

手順

1. ネームサービスキャッシュを有効にしていない場合は、 advanced 権限モードで次のいずれかを実行します。

フラッシュ対象	入力するコマンド
すべてのエクスポートポリシーキャッシュ（showmount を除く）	`vserver export-policy cache flush -vserver vserver_name`
エクスポートポリシールールアクセスキャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache access` オプションのを指定できます `-node` アクセスキャッシュをフラッシュするノードを指定するパラメータ。
ホスト名キャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache host`
ネットグループキャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache netgroup` ネットグループの処理は大量のリソースを消費します。ネットグループキャッシュのフラッシュは、古いネットグループが原因で発生したクライアントアクセス問題の解決を試みる場合にのみ行ってください。
showmount キャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

2. ネームサービスキャッシュが有効になっている場合は、次のいずれかを実行します。

フラッシュ対象	入力するコマンド
エクスポートポリシールールアクセスキャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache access` オプションのを指定できます `-node` アクセスキャッシュをフラッシュするノードを指定するパラメータ。

フラッシュ対象	入力するコマンド
ホスト名キャッシュ	`vserver services name-service cache hosts forward-lookup delete-all`
ネットグループキャッシュ	`vserver services name-service cache netgroups ip-to-netgroup delete-all` `vserver services name-service cache netgroups members delete-all` ネットグループの処理は大量のリソースを消費します。ネットグループキャッシュのフラッシュは、古いネットグループが原因で発生したクライアントアクセス問題の解決を試みる場合にのみ行ってください。
showmount キャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

エクスポートポリシーネットグループのキューとキャッシュを表示します

ONTAP では、ネットグループのインポート時および解決時にネットグループキューを使用し、結果として得られる情報を格納するためにネットグループキャッシュを使用します。エクスポートポリシーのネットグループ関連の問題をトラブルシューティングする場合は、を使用できます `vserver export-policy netgroup queue show` および `vserver export-policy netgroup cache show` ネットグループキューのステータスおよびネットグループキャッシュの内容を表示するコマンド。

ステップ

1. 次のいずれかを実行します。

エクスポートポリシーネットグループに関する表示対象	入力するコマンド
キュー	`vserver export-policy netgroup queue show`
キャッシュ	`vserver export-policy netgroup cache show -vserver vserver_name`

詳細については、各コマンドのマニュアルページを参照してください。

クライアント **IP** アドレスがネットグループのメンバーであるかどうかを確認します

ネットグループに関連するNFSクライアントアクセスの問題をトラブルシューティングする場合は、を使用できます `vserver export-policy netgroup check-membership` クライアントIPが特定のネットグループのメンバーであるかどうかを確認するためのコマンド。

このタスクについて

ネットグループメンバーシップのチェックにより、クライアントがネットグループのメンバーであることまたはメンバーでないことを ONTAP が認識しているかどうかを確認できます。また、ネットグループ情報の更新中に ONTAP ネットグループキャッシュが一時的な状態にあるかどうかもわかります。この情報は、クライアントに対して予期せずアクセスが許可または拒否される理由を理解するのに役立ちます。

ステップ

1. クライアントIPアドレスのネットグループメンバーシップを確認します。 `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   このコマンドによって次のような結果が返されることがあります。

   - クライアントはネットグループのメンバーです。

     これは、リバースルックアップスキャンまたはホスト単位のネットグループ検索によって確認されました。

   - クライアントはネットグループのメンバーです。

     クライアントが ONTAP のネットグループキャッシュに見つかりました。

   - クライアントはネットグループのメンバーではありません。
   - ONTAP が現在ネットグループキャッシュを更新中なので、まだクライアントのメンバーシップを決定できません。

     これが完了するまで、メンバーシップの判断を明示的に下すことはできません。を使用します `vserver export-policy netgroup queue show` ネットグループのロードを監視し、完了後にチェックを再試行するコマンド。

例

次の例は、 IP アドレスが 172.17.16.72 のクライアントが SVM vs1 上のネットグループ mercury のメンバーであるかどうかをチェックします。

```
 cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
```

アクセスキャッシュのパフォーマンスを最適化

複数のパラメータを設定して、アクセスキャッシュを最適化したり、パフォーマンスとアクセスキャッシュに格納される情報の鮮度とのバランスをとったりすることができます。

このタスクについて

アクセスキャッシュの更新期間を設定するときは、次の点に注意してください。

- 値を大きくすると、アクセスキャッシュ内のエントリの保持期間が長くなります。

長所としては、 ONTAP がアクセスキャッシュエントリの更新時に消費するリソースの減少によるパフォーマンスの向上が挙げられます。短所は、エクスポートポリシールールが変更されてアクセスキャッシュエントリが古くなった場合、エントリの更新にかかる時間が長くなることです。その結果、アクセスできるはずのクライアントが拒否され、拒否されるはずのクライアントがアクセス権を取得する可能性があります。

- 値を小さくすると、 ONTAP によるアクセスキャッシュエントリの更新頻度が高くなります。

  長所は、エントリの鮮度が向上し、クライアントに対するアクセスの許可または拒否が正しく行われる可能性が高くなることです。短所としては、 ONTAP がアクセスキャッシュエントリの更新時に消費するリソースの増加によるパフォーマンスの低下が挙げられます。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 必要な操作を実行します。

変更の対象	入力するコマンド
正のエントリの更新期間	`vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value`
負のエントリの更新期間	`vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value`
古いエントリのタイムアウト時間	`vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value`

3. 新しいパラメータ設定を確認します。

   ```
   vserver export-policy access-cache config show-all-vservers
   ```

4. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

ファイルロックを管理します

プロトコル間のファイルロックについて

ファイルロックは、あるユーザが以前に開いていたファイルに別のユーザがアクセスするのを防ぐために、クライアントアプリケーションで使用される方法です。ONTAP でファイルをロックする方法は、クライアントのプロトコルによって異なります。

クライアントが NFS クライアントである場合、ロックは任意に設定します。クライアントが SMB クライアントである場合、ロックは必須となります。

NFS ファイルと SMB ファイルのロックの違いのため、 SMB アプリケーションですでに開いているファイルに NFS クライアントからアクセスすると、エラーになる場合があります。

NFS クライアントが SMB アプリケーションによってロックされたファイルにアクセスすると、次のいずれかの状態になります。

- mixed形式またはNTFS形式のボリュームでは、などのファイル操作が行われます `rm`、 `rmdir`および `mv` NFSアプリケーションが失敗するように原因 できますか。
- NFS の読み取りと書き込みの処理は、 SMB の読み取り拒否および書き込み拒否のオープンモードによってそれぞれ拒否されます。
- また、ファイルの書き込み対象となる範囲が、排他的な SMB バイトロックでロックされている場合も、 NFS の書き込みの処理はエラーになります。

UNIX セキュリティ形式のボリュームでは、 NFS のリンク解除および名前変更の処理で SMB のロック状態が無視され、ファイルへのアクセスが許可されます。UNIX セキュリティ形式のボリュームでのその他すべての NFS 処理では、 SMB のロック状態が考慮されます。

ONTAP による読み取り専用ビットの処理方法

読み取り専用ビットは、ファイルが書き込み可能（無効）なのか読み取り専用（有効）なのかを示すために、ファイルごとに設定されます。

Windows を使用する SMB クライアントは、ファイルごとの読み取り専用ビットを設定できます。NFS クライアントは、ファイルごとの読み取り専用ビットを設定しません。 NFS クライアントは、ファイルごとの読み取り専用ビットを使用するプロトコル操作を行わないためです。

ONTAP は、 Windows を使用する SMB クライアントによってファイルが作成される際に、そのファイルに読み取り専用ビットを設定できます。ファイルが NFS クライアントと SMB クライアント間で共有されている場合も、 ONTAP は読み取り専用ビットを設定できます。一部のソフトウェアは、 NFS クライアントおよび SMB クライアントで使用される場合、読み取り専用ビットが有効になっている必要があります。

NFS クライアントと SMB クライアント間で共有されるファイルに対して、適切な読み取りおよび書き込み権限を保持するために、読み取り専用ビットが次の規則に従って処理されます。 ONTAP

- NFS は、読み取り専用ビットが有効になっているファイルを書き込み権限ビットが無効になっているファイルとして扱います。
- NFS クライアントがすべての書き込み権限ビットを無効にしたときに、これらのうち少なくとも 1 つが以前有効であったら、 ONTAP はそのファイルの読み取り専用ビットを有効にします。
- NFS クライアントがすべての書き込み権限ビットを有効にすると、 ONTAP はそのファイルの読み取り専用ビットを無効にします。
- あるファイルの読み取り専用ビットが有効になっているときに、 NFS クライアントがそのファイルの権限を調べようとすると、そのファイルの権限ビットは NFS クライアントには送信されず、代わりに書き込み権限ビットがマスクされた権限ビットが ONTAP クライアントに送信されます。
- ファイルの読み取り専用ビットが有効になっているときに、 SMB クライアントがこの読み取り専用ビットを無効にすると、 ONTAP はそのファイルに対する所有者の書き込み権限ビットを有効にします。
- 読み取り専用ビットが有効になっているファイルに書き込めるのは、 root のみです。

ファイル権限の変更は、 SMB クライアントではすぐに反映されますが、 NFS クライアントが属性のキャッシュを有効にしている場合は NFS クライアントではすぐに反映されないことがあります。

共有パスコンポーネントのロックの処理に関する **ONTAP** と **Windows** の違い

Windows とは異なり、 ONTAP では、ファイルが開いているときにそのファイルのパスの各コンポーネントがロックされません。この動作は SMB 共有パスにも影響します。

ONTAP 原因ではパスの各コンポーネントがロックされないため、開いているファイルまたは共有より上のパスコンポーネントの名前を変更できます。このため、特定のアプリケーションで原因の問題が発生したり、SMB 構成の共有パスを無効な名前に変更したりすることができます。原因によって共有にアクセスできなくなる可能性があります。

パスコンポーネントの名前変更による問題を回避するには、Windows Access Control List（ACL；アクセス制御リスト）のセキュリティ設定を適用して、ユーザやアプリケーションが重要なディレクトリの名前を変更できないようにします。

の詳細を確認してください "クライアントがアクセスしている間にディレクトリの名前を変更しないようにする方法"。

ロックに関する情報を表示します

有効になっているロックの種類とロックの状態、バイト範囲ロック、共有ロックモード、委譲ロック、および便宜的ロックの詳細、永続性ハンドルを使用してロックが開かれているかどうかなど、現在のファイルロックに関する情報を表示できます。

このタスクについて

NFSv4 または NFSv4.1 を使用して確立されたロックについては、クライアント IP アドレスを表示できません。

デフォルトでは、すべてのロックに関する情報が表示されます。コマンドパラメータを使用すると、特定の Storage Virtual Machine （ SVM ）のロックに関する情報を表示したり、他の条件によってコマンドの出力をフィルタリングしたりできます。

。 `vserver locks show` コマンドは、次の4種類のロックに関する情報を表示します。

- バイト範囲ロック。ファイルの一部のみをロックします。
- 共有ロック。開いているファイルをロックします。
- 便宜的ロック。 SMB を使用してクライアント側キャッシュを制御します。
- 委譲。 NFSv4.x を使用してクライアント側キャッシュを制御します

オプションのパラメータを指定すると、各ロックタイプに関する重要な情報を確認できます。詳細については、コマンドのマニュアルページを参照してください。

ステップ

1. を使用して、ロックに関する情報を表示します `vserver locks show` コマンドを実行します

例

次の例は、パスのファイルに対するNFSv4ロックに関する概要情報を表示します `/vol1/file1`。共有ロックのアクセスモードは write-deny_none であり、書き込み委譲でロックが許可されています。

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path                LIF         Protocol  Lock Type   Client
------- -------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1                lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                          delegation  -
               Delegation Type: write
```

次の例は、パスのファイルに対するSMBロックに関するoplockおよび共有ロックの詳細情報を表示します `/data2/data2_2/intro.pptx`。IP アドレスが 10.3.1.3 のクライアントに対して、共有ロックのアクセスモードを write-deny_none として、永続性ハンドルが許可されています。バッチの oplock レベルで oplock リースが許可されています。

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
```

```
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                    Vserver: vs1
                     Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/test.pptx
                 Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

ロックを解除します

ファイルロックが原因でクライアントがファイルにアクセスできなくなっている場合は、現在有効なロックの情報を表示して、特定のロックを解除することができます。ロックの解除が必要になるケースとしては、アプリケーションのデバッグなどが挙げられます。

このタスクについて

。 `vserver locks break` コマンドは、advanced権限レベル以上でのみ使用できます。詳細については、コマンドのマニュアルページを参照してください。

手順

1. ロックを解除するために必要な情報を確認するには、を使用します `vserver locks show` コマンドを実行します

   詳細については、コマンドのマニュアルページを参照してください。

2. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

3. 次のいずれかを実行します。

ロックを解除するための指定項目	入力するコマンド
SVM 名、ボリューム名、 LIF 名、およびファイルパス	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
ロック ID	`vserver locks break -lockid UUID`

4. admin 権限レベルに戻ります。

```
set -privilege admin
```

NFS での FPolicy の first-read および first-write フィルタの動作

外部 FPolicy サーバを使用して FPolicy が有効になっていて、読み取り / 書き込み処理が監視対象イベントの場合、読み取り / 書き込み要求のトラフィックが多いと NFS クライアントで応答時間が長くなります。NFS クライアントの場合、 FPolicy で first-read フィルタと first-write フィルタを使用すると、 FPolicy 通知の数が減り、パフォーマンスが向上します。

NFS では、クライアントはファイルに対して I/O を実行する際に、ファイルのハンドルを取得します。このハンドルは、サーバとクライアントのリブート後も有効なままになる場合があります。このため、クライアントはハンドルを自由にキャッシュし、ハンドルを再取得しなくてもハンドルに対する要求を送信できます。通常のセッションでは、大量の読み取り / 書き込み要求がファイルサーバに送信されます。これらのすべての要求について通知が生成されると、次の問題が発生する可能性があります。

- 追加の通知処理により負荷が増大し、応答時間が長くなります。
- サーバに影響のない通知も含め、多数の通知が FPolicy サーバに送信される。

クライアントから特定のファイルに対する最初の読み取り / 書き込み要求を受信すると、キャッシュエントリが作成され、読み取り / 書き込みの数が増分されます。この要求は初回読み取り / 書き込み処理とマークされ、 FPolicy イベントが生成されます。NFS クライアント用の FPolicy フィルタを計画して作成する前に、FPolicy フィルタの基本的な仕組みを理解しておく必要があります。

- first-read ：初回読み取りのクライアント要求をフィルタリングします。

  このフィルタはNFSイベントに使用されます `-file-session-io-grouping-count` および `-file-session-io-grouping-duration` FPolicyが処理される初回読み取り要求は、設定によって決まります。

- first-write ：初回書き込みのクライアント要求をフィルタリングします。

  このフィルタはNFSイベントに使用されます `-file-session-io-grouping-count` および `-file-session-io-grouping-duration` 設定により、FPolicyが処理された初回書き込み要求が決まります。

NFS サーバのデータベースには、次のオプションが追加されます。

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

NFSv4.1 サーバ実装 ID を変更する

NFSv4.1 プロトコルには、サーバのドメイン、名前、および日付を記録したサーバ実装 ID が含まれています。サーバ実装 ID のデフォルト値は変更できます。デフォルト値を変更すると、たとえば、使用率の統計を収集したり、相互運用性の問題をトラブルシューティングしたりするときに役立ちます。詳細については、 RFC 5661 を参照してください。

このタスクについて

3 つのオプションのデフォルト値は次のとおりです。

オプション	オプション名	デフォルト値
NFSv4.1 実装 ID - ドメイン	`-v4.1-implementation -domain`	NetApp.com にアクセスします
NFSv4.1 実装 ID の名前	`-v4.1-implementation-name`	クラスタバージョンの名前
NFSv4.1 実装 ID - 日付	`-v4.1-implementation-date`	クラスタバージョンの日付

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

変更する **NFSv4.1** 実装 **ID** のオプション	入力するコマンド
ドメイン	`vserver nfs modify -v4.1 -implementation-domain domain`
名前	`vserver nfs modify -v4.1 -implementation-name name`

変更する **NFSv4.1** 実装 **ID** のオプション	入力するコマンド
日付	`vserver nfs modify -v4.1 -implementation-date date`

3. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

NFSv4 ACLs を管理します

NFSv4 ACL を有効化する利点

NFSv4 ACL を有効化すると多くの利点を得られます。

NFSv4 ACL を有効にする利点は次のとおりです。

- ファイルやディレクトリへのユーザアクセスのより詳細な制御
- NFS セキュリティが向上します
- CIFS との相互運用性の向上
- NFS のユーザあたりの最大グループ数は 16 ではなくなりました

NFSv4 ACL の仕組み

NFSv4 ACL を使用しているクライアントは、システム上のファイルとディレクトリに ACL を設定し、その ACL を表示することができます。ACL が設定されているディレクトリ内にファイルやサブディレクトリを新しく作成すると、新しいファイルやサブディレクトリには、その ACL 内の ACE のうち、該当する継承フラグが指定された ACL エントリ（ACE ）がすべて継承されます。

ファイルやディレクトリが NFSv4 要求によって作成される場合、作成されるファイルやディレクトリの ACL は、ファイル作成要求に ACL が含まれているか、または標準の UNIX ファイルアクセス権限のみが含まれているか、および親ディレクトリに ACL が設定されているかどうかによって異なります。

- 要求に ACL が含まれる場合は、その ACL が使用されます。
- 要求に標準 UNIX ファイルアクセス権限のみが含まれ、親ディレクトリに ACL がある場合、親ディレクトリの ACL の ACE に適切な継承フラグのタグが付けられていれば、それらの ACE が新しいファイルやディレクトリに継承されます。

  > 親ACLは、の場合でも継承されます `-v4.0-acl` がに設定されます `off`。

- 要求に標準の UNIX ファイルアクセス権限のみが含まれ、親ディレクトリに ACL がない場合は、クライアントのファイルモードを使用して標準の UNIX ファイルアクセス権限が設定されます。
- 要求に標準 UNIX ファイルアクセス権限のみが含まれ、親ディレクトリに継承できない ACL がある場合は、モードビットのみを使用して新しいオブジェクトが作成されます。

状況に応じて `-chown-mode` パラメータがに設定されました `restricted` でコマンドを使用します `vserver nfs` または `vserver export-policy rule` ファミリーの場合、NFSv4 ACLで設定されたディスク上の権限でroot以外のユーザがファイル所有権を変更できる場合でも、スーパーユーザのみがファイル所有権を変更できます。詳細については、関連するマニュアルページを参照してください。

NFSv4 ACL の変更を有効または無効にします

ONTAP がを受信したとき `chmod` ACLが設定されたファイルまたはディレクトリに対するコマンド。デフォルトでは、ACLは保持され、モードビットの変更を反映するように変更されます。を無効にすることができます `-v4-acl-preserve` 代わりにACLをドロップする場合に動作を変更するパラメータ。

このタスクについて

unified セキュリティ形式を使用している場合、このパラメータは、クライアントがファイルまたはディレクトリに対する chmod 、 chgroup 、または chown コマンドを送信したときに NTFS ファイルアクセス権が保持されるか破棄されるかの指定も行います。

このパラメータのデフォルトは enabled です。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

状況	入力するコマンド
既存の NFSv4 ACL の保持と変更を有効にする（デフォルト）	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
保持を無効にして、モードビットを変更するときに NFSv4 ACL を破棄します	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

ONTAP での **NFSv4 ACL** を使用したファイル削除の可否の判別方法

ファイルを削除できるかどうかを判別するために、 ONTAP は、そのファイルの DELETE ビットと、ファイルが含まれるディレクトリの DELETE_CHILD ビットの組み合わせを使用します。詳細については、 NFS 4.1 RFC 5661 を参照してください。

NFSv4 ACL を有効または無効にします

NFSv4 ACLを有効または無効にするには、を変更します `-v4.0-acl` および `-v4.1-acl` オプション（ Options ）これらのオプションは、デフォルトでは無効になっています。

このタスクについて

。 `-v4.0-acl` または `-v4.1-acl` オプションは、NFSv4 ACLの設定と表示を制御します。アクセスチェックでのNFSv4 ACLの適用は制御しません。

ステップ

1. 次のいずれかを実行します。

状況	作業
NFSv4.0 ACL を有効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
NFSv4.0 ACL を無効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
NFSv4.1 ACLを有効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`
NFSv4.1 ACLを無効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

NFSv4 ACL の **ACE** の最大数を変更する

パラメータを変更すると、各NFSv4 ACLに許可されるACEの最大数を変更できます `-v4-acl-max-aces`。デフォルトでは、 ACL あたりの ACE の数は 400 個に制限されています。この制限を引き上げることで、 400 個を超える ACE を含む ACL のデータを、ONTAP を実行するストレージシステムに移行できるようになります。

このタスクについて

この制限値を増やすと、 NFSv4 ACL を含むファイルにアクセスするクライアントのパフォーマンスが低下することがあります。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. NFSv4 ACL の ACE の最大数を変更します。

   ```
   vserver nfs modify -v4-acl-max-aces max_ace_limit
   ```

   の有効な範囲

   `max_ace_limit` はです `192` 終了： `1024.`

3. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

NFSv4 ファイル委譲を管理します

NFSv4 読み取りファイル委譲を有効または無効にします

NFSv4読み取りファイル委譲を有効または無効にするには、を変更します `-v4.0-read-delegation`または オプション読み取りファイル委譲を有効にすると、ファイルのオープンとクローズに伴うメッセージのオーバーヘッドを大幅に軽減できます。

このタスクについて

デフォルトでは、読み取りファイル委譲は無効です。

読み取りファイル委譲を有効にした場合の欠点は、サーバのリブートまたはリスタート後、クライアントのリブートまたはリスタート後、あるいはネットワークを分割したあとに、サーバおよびそのクライアントが委譲をリカバリする必要があることです。

ステップ

1. 次のいずれかを実行します。

状況	作業
NFSv4 読み取りファイル委譲を有効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled`
NFSv4.1 読み取りファイル委譲を有効にします	次のコマンドを入力します。 [+] `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled`

NFSv4 読み取りファイル委譲を無効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled`
NFSv4.1読み取りファイル委譲を無効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled`

結果

ファイル委譲オプションの変更はすぐに反映されます。NFS のリブートやリスタートは必要ありません。

NFSv4 書き込みファイル委譲を有効または無効にします

書き込みファイル委譲を有効または無効にするには、を変更します `-v4.0-write-delegation`または オプション書き込みファイル委譲を有効にすると、ファイルのオープンとクローズだけでなく、ファイルおよびレコードのロックに関連するメッセージのオーバーヘッドを大幅に軽減できます。

このタスクについて

デフォルトでは、書き込みファイル委譲は無効です。

書き込みファイル委譲を有効にした場合の欠点は、サーバのリブートまたはリスタート後、クライアントのリブートまたはリスタート後、あるいはネットワークを分割したあとに、サーバおよびそのクライアントが委譲をリカバリするための追加タスクを実行する必要があることです。

ステップ

1. 次のいずれかを実行します。

状況	作業
NFSv4 書き込みファイル委譲を有効にします	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled`
NFSv4.1書き込みファイル委譲を有効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled`
NFSv4 書き込みファイル委譲を無効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled`

状況	作業
NFSv4.1 書き込みファイル委譲を無効にします	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled`

結果

ファイル委譲オプションの変更はすぐに反映されます。NFS のリブートやリスタートは必要ありません。

NFSv4 ファイルおよびレコードロックを設定する

NFSv4 ファイルおよびレコードロックについて

NFSv4 クライアントの場合、 ONTAP は NFSv4 のファイルロックメカニズムをサポートしているため、すべてのファイルのロック状態がリースベースモデルで保持されます。

"ネットアップテクニカルレポート 3580 ：『 NFSv4 の拡張内容とベスト・プラクティス・ガイド - Data ONTAP での実装』"

NFSv4 ロックリース期間を指定します

NFSv4ロックリース期間（ONTAP がクライアントに解除不能なロックを付与する期間）を指定するには、を変更します `-v4-lease-seconds` オプションリース期間を短くするとサーバのリカバリにかかる時間が短縮され、リース期間を長くすると、大量のクライアントを処理するサーバに効果的です。

このタスクについて

デフォルトでは、このオプションはに設定されています `30`。このオプションの最小値はです `10`。このオプションの最大値はロック猶予期間です。この期間は、で設定できます `locking.lease_seconds` オプション

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 次のコマンドを入力します。

   ```
   vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
   ```

3. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

NFSv4 ロック猶予期間を指定します

NFSv4ロック猶予期間（サーバリカバリ中にクライアントがロック状態をONTAP に再

要求する期間）を指定するには、を変更します `-v4-grace-seconds` オプション

このタスクについて

デフォルトでは、このオプションはに設定されています `45`。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 次のコマンドを入力します。

   ```
   vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
   ```

3. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

NFSv4 リファーラルの仕組み

NFSv4 リファーラルを有効にすると、 ONTAP は NFSv4 クライアントに対して「 SVM 内」のリファーラルを提供します。SVM 内リファーラルでは、 NFSv4 要求を受け取ったクラスタノードが、 NFSv4 クライアントに Storage Virtual Machine （ SVM ）の別の論理インターフェイス（ LIF ）を紹介します。

NFSv4 クライアントは、それ以降、ターゲット LIF でリファーラルを受け取ったパスにアクセスする必要があります。元のクラスタノードがこのようなリファーラルを返すのは、データボリュームが存在するクラスタノード上の SVM に LIF があるため、クライアントがデータにより高速にアクセスでき、余分なクラスタ通信が回避されると判断された場合です。

NFSv4 リファーラルを有効または無効にします

Storage Virtual Machine（SVM）でNFSv4リファーラルを有効にするには、オプションを有効にします `-v4-fsid-change` および `-v4.0-referrals`または。NFSv4 リファーラルを有効にすると、この機能をサポートする NFSv4 クライアントのデータへのアクセス速度を向上させることができます。

必要なもの

NFS リファーラルを有効にする場合は、まず Parallel NFS を無効にする必要があります。両方を同時に有効にすることはできません。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

状況	入力するコマンド
NFSv4 リファーラルを有効にする	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled` `vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
NFSv4 リファーラルを無効にする	`vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled`
NFSv4.1リファーラルを有効にする	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled` `vserver nfs modify -vserver vserver_name -v4.1-referrals enabled`
NFSv4.1リファーラルを無効にする	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

NFS統計の表示

パフォーマンスを監視して問題を診断するために、ストレージシステム上の Storage Virtual Machine （ SVM ）の NFS 統計を表示することができます。

手順

1. を使用します `statistics catalog object show` コマンドを使用して、データを表示できるNFSオブジェクトを特定します。

   ```
   statistics catalog object show -object nfs*
   ```

2. を使用します `statistics start` およびオプションです `statistics stop` 1つ以上のオブジェクトからデータサンプルを収集するコマンド。
3. を使用します `statistics show` コマンドを使用してサンプルデータを表示します。

例：**NFSv3**のパフォーマンスの監視

次の例は、 NFSv3 プロトコルのパフォーマンスデータを表示します。

次のコマンドは、新しいサンプルのデータ収集を開始します。

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

次のコマンドは、正常に行われた読み取り要求および書き込み要求の数と読み取り要求と書き込み要求の総数を比較するカウンタを指定して、サンプルからデータを表示します。

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                             Value
    --------------------------- ---------------------------
    read_success                                        40042
    read_total                                          40042
    write_success                                     1492052
    write_total                                       1492052
```

関連情報

"パフォーマンス監視のセットアップ"

DNS統計を表示します。

パフォーマンスを監視して問題を診断するために、ストレージシステム上のStorage Virtual Machine（SVM）のDNS統計を表示することができます。

手順

1. を使用します `statistics catalog object show` コマンドを使用して、データを表示できるDNSオブジェクトを特定します。

   ```
   statistics catalog object show -object external_service_op*
   ```

2. を使用します `statistics start` および `statistics stop` 1つ以上のオブジェクトからデータサンプルを収集するコマンド。
3. を使用します `statistics show` コマンドを使用してサンプルデータを表示します。

DNS 統計を監視しています

次の例は、 DNS クエリのパフォーマンスデータを表示します。次のコマンドは、新しいサンプルのデータ収集を開始します。

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

次のコマンドは、送信した DNS クエリの数と、受信した / 失敗した / タイムアウトになった DNS クエリの数

を比較するカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- ---------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            0
    num_requests_sent                                               1
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

次のコマンドは、特定のサーバの DNS クエリに対して特定のエラーを受信した回数を示すカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- ---------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                  10.72.219.109
3 entries were displayed.
```

関連情報

"パフォーマンス監視のセットアップ"

NIS統計を表示する

パフォーマンスを監視して問題を診断するために、ストレージシステム上のStorage Virtual Machine（SVM）のNIS統計を表示することができます。

手順

1. を使用します `statistics catalog object show` コマンドを使用して、データを表示できるNISオブジェクトを特定します。

   ```
   statistics catalog object show -object external_service_op*
   ```

2. を使用します `statistics start` および `statistics stop` 1つ以上のオブジェクトからデータサンプルを収集するコマンド。
3. を使用します `statistics show` コマンドを使用してサンプルデータを表示します。

NIS 統計を監視する

次の例は、 NIS クエリのパフォーマンスデータを表示します。次のコマンドは、新しいサンプルのデータ収集を開始します。

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

次のコマンドは、送信した NIS クエリの数と、受信した / 失敗した / タイムアウトになった NIS クエリの数を比較するカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            1
    num_requests_sent                                               2
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

次のコマンドは、特定のサーバの NIS クエリに対して特定のエラーを受信した回数を示すカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                           YP_NOTFOUND
    server_ip_address                                    10.227.13.221
3 entries were displayed.
```

関連情報

"パフォーマンス監視のセットアップ"

VMware vStorage over NFS がサポートされるようになりました

ONTAP は、 NFS 環境で特定の VMware vStorage API for Array Integration （ VAAI ）機能をサポートしています。

サポートされている機能

次の機能がサポートされます。

- コピーオフロード

  ESXi ホストで、仮想マシンや仮想マシンディスク（ VMDK ）のコピーを、ホストを介さずにソースとデスティネーションのデータストア間で直接実行できます。これにより、 ESXi ホストの CPU サイクルやネットワーク帯域幅を節約できます。ソースボリュームがスパースボリュームの場合、コピーオフロードでスペース効率が保持されます。

- スペースリザベーション

  スペースをリザーブして VMDK ファイル用のストレージスペースを確保します。

制限

NFS で VMware vStorage を使用する際には、次の制限事項があります。

- 次の場合にコピーオフロード処理が失敗することがあります。
  - ソースボリュームまたはデスティネーションボリュームで wafliron を実行中に、ボリュームが一時的にオフラインになっている
  - ソースボリュームまたはデスティネーションボリュームを移動しているとき
  - ソースまたはデスティネーションの LIF を移動しているとき
  - テイクオーバーまたはギブバック処理を実行しているとき
  - スイッチオーバーまたはスイッチバック処理を実行しているとき
- 次のシナリオでは、ファイルハンドル形式の違いが原因でサーバ側のコピーが失敗する可能性があります。

  qtree のエクスポートを現在行っているか、以前行っていた SVM から、これまでに qtree をエクスポートしたことがない SVM へのデータのコピーを試みます。上記の制限を回避するために、デスティネーション SVM で少なくとも 1 つの qtree をエクスポートすることができます。

関連情報

"Data ONTAP では、 VAAI オフロード処理はどのようにサポートされていますか。"

VMware vStorage over NFS を有効または無効にします

を使用して、Storage Virtual Machine（SVM）でVMware vStorage over NFSのサポートを有効または無効にできます `vserver nfs modify` コマンドを実行します

このタスクについて

デフォルトでは、 VMware vStorage over NFS のサポートは無効になっています。

手順

1. SVM での現在の vStorage のサポートステータスを表示します。

```
vserver nfs show -vserver vserver_name -instance
```

2. 次のいずれかを実行します。

状況	入力するコマンド
VMware vStorage のサポートを有効にします	`vserver nfs modify -vserver vserver_name -vstorage enabled`
VMware vStorage のサポートを無効にします	`vserver nfs modify -vserver vserver_name -vstorage disabled`

完了後

この機能を使用する前に、 NFS Plug-in for VMware VAAI をインストールしておく必要があります。詳細については、「 NetApp NFS Plug-in for VMware VAAI のインストール」を参照してください。

関連情報

"ネットアップのマニュアル： NetApp NFS Plug-in for VMware VAAI"

rquota のサポートを有効または無効にします

ONTAP は、 remote quota protocol バージョン 1 （ rquota v1 ）をサポートしています。rquota プロトコルを使用すると、 NFS クライアントは、リモートマシンからユーザのクォータ情報を取得できます。Storage Virtual Machine（SVM）でrquotaを有効にするには、を使用します `vserver nfs modify` コマンドを実行します

このタスクについて

デフォルトでは、 rquota は無効です。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
SVM で rquota のサポートを有効にします	`vserver nfs modify -vserver vserver_name -rquota enable`
SVM で rquota のサポートを無効にします	`vserver nfs modify -vserver vserver_name -rquota disable`

クォータの詳細については、を参照してください "論理ストレージ管理"。

TCP 転送サイズを変更することで NFSv3 / NFSv4 のパフォーマンスが向上します

TCP 最大転送サイズを変更することで、高レイテンシのネットワーク経由でストレージシステムに接続する NFSv3 / NFSv4 クライアントのパフォーマンスを向上させることができます。

レイテンシが 10 ミリ秒を超えるワイドエリアネットワーク（ WAN ）またはメトロエリアネットワーク（ MAN ）などの高レイテンシネットワークを介してクライアントがストレージシステムにアクセスしている場合は、 TCP 最大転送サイズを変更することで、ネットワーク接続のパフォーマンスを向上させることができます。ローカルエリアネットワーク（ LAN ）などの低レイテンシネットワークでストレージシステムにアクセスするクライアントは、これらのパラメータを変更してもパフォーマンスの向上はあまり期待できません。スループットの向上がレイテンシの影響を上回らない場合は、これらのパラメータを使用しないでください。

ストレージ環境がこれらのパラメータの変更の恩恵を受けるかどうかを判断するには、まずパフォーマンスの低い NFS クライアントで総合的なパフォーマンス評価を行ってください。パフォーマンスの低さが、クライアント上の過剰なラウンドトリップによるレイテンシとデータ量の少ない要求によるものかどうかを確認します。このような状況では、クライアントとサーバは、接続を介して送信される小さな要求と応答を待機するデューティサイクルの大部分を消費するため、使用可能な帯域幅を完全に使用することはできません。

NFSv3 と NFSv4 の要求サイズを大きくすることで、クライアントとサーバは使用可能な帯域幅をより効果的に使用できるようになり、単位時間あたりの移動データ量が多くなります。そのため、接続の全体的な効率が向上します。

ストレージシステムとクライアントの間で設定が異なる場合があることに注意してください。ストレージシステムとクライアントでサポートされる転送処理の最大サイズは 1MB です。ただし、ストレージシステムで最大転送サイズを 1MB に設定しても、クライアントがサポートするサイズが 64KB であると、マウントの転送サイズは 64KB 以下に制限されます。

これらのパラメータを変更する前に注意しなければならないのは、変更すると、大量の応答をアセンブルして送信するのに時間がかかり、ストレージシステムでメモリ消費が増えるということです。ストレージシステムへの高レイテンシ接続が増えるほど、メモリ消費量も増加します。メモリ容量が多いストレージシステムでは、この変更による影響はほとんどありません。メモリ容量が少ないストレージシステムでは、パフォーマンスが著しく低下する可能性があります。

これらのパラメータを効果的に使用するには、クラスタの複数のノードからデータを取得する必要があります。クラスタネットワーク固有のレイテンシによって、応答の全体的なレイテンシが増加する可能性があります。これらのパラメータを使用するときに、全体的なレイテンシが増大する傾向があります。そのため、レイテンシの影響を受けやすいワークロードは悪影響を受ける可能性があります。

NFSv3 と NFSv4 の TCP 最大転送サイズを変更する

を変更できます `-tcp-max-xfer-size` NFSv3およびNFSv4.xプロトコルを使用するすべてのTCP接続の最大転送サイズを設定するオプション。

このタスクについて

これらのオプションは Storage Virtual Machine （ SVM ）ごとに変更できます。

ONTAP 9以降では、を参照してください `v3-tcp-max-read-size` および `v3-tcp-max-write-size` オプションは廃止されました。を使用する必要があります `-tcp-max-xfer-size` 代わりにオプション。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

状況	入力するコマンド
NFSv3 または NFSv4 の TCP 最大転送サイズを変更する	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

オプション	範囲	デフォルト
`-tcp-max-xfer-size`	8192~1048576 バイト	65536バイト

> 最大転送サイズには、 4KB （ 4096 バイト）の倍数を入力する必要があります。要求が要件を満たしていない場合は、パフォーマンスが低下します。

3. を使用します `vserver nfs show -fields tcp-max-xfer-size` コマンドを使用して変更を確認します。
4. 静的マウントを使用しているクライアントがある場合、新しいパラメータサイズを有効にするには、いったんアンマウントしてから再度マウントします。

例

次のコマンドは、 vs1 という SVM で NFSv3 と NFSv4.x の TCP 最大転送サイズを 1 、 048 、 576 バイトに設定します。

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

NFS ユーザに許可するグループ ID の数を設定します

ONTAP は、 Kerberos （ RPCSEC_GSS ）認証を使用して NFS ユーザクレデンシャルを処理する場合、デフォルトで最大 32 個のグループ ID をサポートしています。AUTH_SYS 認証を使用する場合は、 RFC 5331 で定義されているとおり、グループ ID のデフォルトの最大数は 16 個です。デフォルト数を超えるグループに属しているユーザがいる場合は、この最大数を 1 、 024 まで増やすことができます。

このタスクについて

デフォルト数を超えるグループ ID がクレデンシャルに設定されている場合、残りのグループ ID は切り捨てられ、そのユーザがストレージシステムのファイルにアクセスしようとするとエラーが発生する可能性があります。SVM あたりの最大グループ数は、環境内の最大グループ数と同じ数に設定する必要があります。

次の表に、の2つのパラメータを示します `vserver nfs modify` 3つの設定例でグループIDの最大数を決定するコマンド。

パラメータ	設定	結果として得られるグループ ID の上限数

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`32`
	
	`disabled`
	
	これらはデフォルト設定です。
		RPCSEC_GSS ： 32
		
		AUTH_SYS ： 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`256`
	
	`disabled`
		RPCSEC_GSS：256
		
		AUTH_SYS ： 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`512`
	
	`enabled`
		RPCSEC_GSS：512
		
		AUTH_SYS：512

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 必要な操作を実行します。

許可される補助グループの最大数の設定対象	入力するコマンド
RPCSEC_GSS の場合のみ、 AUTH_SYS はデフォルト値の 16 に設定されます	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`
RPCSEC_GSS と AUTH_SYS の両方	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`

3. を確認します `-extended-groups-limit` AUTH_SYSが拡張グループを使用しているかどうかを確認します。 `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`

4. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

例

次の例は、拡張されたグループを AUTH_SYS 認証で有効にし、 AUTH_SYS 認証と RPCSEC_GSS 認証の両方で拡張グループの最大数を 512 に設定します。これらの変更は、 vs1 という SVM にアクセスするクライアントに対してのみ行われます。

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ ---------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

NTFS セキュリティ形式のデータへの root ユーザアクセスを制御する

NTFS セキュリティ形式のデータへの NFS クライアントアクセスを許可したり、 NTFS クライアントによる NFS セキュリティ形式データへのアクセスを許可したりするように ONTAP を設定することができます。NFS データストアで NTFS セキュリティ形式を使用する際には、 root ユーザによるアクセスの処理方法を決定し、それに応じて Storage Virtual Machine （ SVM ）を設定する必要があります。

このタスクについて

root ユーザが NTFS セキュリティ形式のデータにアクセスする際には、次の 2 つのオプションがあります。

- 他の NFS ユーザと同様に root ユーザを Windows ユーザにマッピングし、 NTFS ACL に従ってアクセスを管理する。
- NTFS ACL を無視してフルアクセスを root に対して提供する。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 必要な操作を実行します。

root ユーザへの対処方法	入力するコマンド
Windows ユーザにマッピングする	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`
NT ACL チェックをバイパスします	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

デフォルトでは、このパラメータは無効になっています。

このパラメータが有効になっていても root ユーザに対するネームマッピングが存在しない場合、 ONTAP はデフォルトの SMB 管理者のクレデンシャルを監査に使用します。

3. admin 権限レベルに戻ります。

```
set -privilege admin
```

サポート対象の**NFS**バージョンとクライアント

サポートされる**NFS**のバージョンとクライアントの概要

ネットワークで NFS を使用する前に、 ONTAP でサポートされる NFS のバージョンとクライアントを確認しておく必要があります。

この表は、NFSプロトコルのメジャーバージョンとマイナーバージョンがONTAP でデフォルトでサポートされる場合を示しています。デフォルトでは、このNFSプロトコルをサポートするONTAP の最も古いバージョンがサポートされているわけではありません。

バージョン	デフォルトは有効です
NFSv3	はい。
NFSv4.0	はい、 ONTAP 9.9.1 以降でサポートされています
NFSv4.1	はい、 ONTAP 9.9.1 以降でサポートされています
NFSv4.2	はい、 ONTAP 9.9.1 以降でサポートされています
pNFS	いいえ

ONTAP でサポートされる NFS クライアントに関する最新情報については、 Interoperability Matrix を参照してください。

"NetApp Interoperability Matrix Tool で確認できます"

ONTAP でサポートされる **NFSv4.0** の機能

ONTAP は、 SPKM3 および LIPKEY のセキュリティ機能を除く NFSv4.0 の必須機能をすべてサポートしています。

次の NFSv4 機能がサポートされます。

- * コンパウンド *

  クライアントは、 1 つのリモート手順呼び出し（ RPC ）要求で複数のファイル操作を要求できます。

- * ファイル委譲 *

  サーバは、一部のタイプのクライアントにファイル制御を委譲して読み取りおよび書き込みアクセスを許可します。

- * 擬似 fs *

  NFSv4 サーバでストレージシステム上のマウントポイントの決定に使用します。NFSv4 にはマウントプロトコルはありません。

- * ロック *

  リースベース。NFSv4 には独立した Network Lock Manager （ NLM ；ネットワークロックマネージャ）または Network Status Monitor （ NSM ；ネットワークステータスモニタ）プロトコルはありません。

NFSv4.0 プロトコルの詳細については、 RFC 3530 を参照してください。

NFSv4 の ONTAP サポートの制限事項

NFSv4 の ONTAP サポートにはいくつかの制限があることに注意してください。

- 委譲機能はすべてのクライアントタイプでサポートされているわけではありません。
- ONTAP 9.4 以前のリリースでは、 UTF8 以外のボリュームで ASCII 以外の文字が含まれている名前はストレージシステムで拒否されます。

  ONTAP 9.5 以降のリリースでは、 utf8mb4 言語設定で作成され NFSv4 を使用してマウントされたボリュームはこの制限を受けなくなります。

- すべてのファイルハンドルは永続的です。サーバは揮発性のファイルハンドルを提供しません。
- 移行とレプリケーションはサポートされていません。
- NFSv4 クライアントは、読み取り専用負荷共有ミラーでサポートされていません。

  ONTAP は、 NFSv4 クライアントを直接読み取りおよび書き込みアクセスの負荷共有ミラーのソースにルーティングします。

- 名前付き属性はサポートされていません。
- 次の属性を除くすべての推奨属性がサポートされています。
  - `archive`
  - `hidden`
  - `homogeneous`
  - `mimetype`
  - `quota_avail_hard`
  - `quota_avail_soft`
  - `quota_used`
  - `system`

- `time_backup`

> ただし、はサポートされていません `quota*` 属性では、ONTAP はRQUOTA側のバンドプロトコルを介してユーザクォータとグループクォータをサポートします。

ONTAP での NFSv4.1 のサポート

ONTAP 9.8 以降では、 NFSv4.1 が有効になっている場合、 nconnect 機能がデフォルトで使用できます。

以前の NFS クライアント実装では、マウントを使用する TCP 接続は 1 つだけです。ONTAP では、 1 つの TCP 接続が IOPS の増加に伴うボトルネックになることがあります。ただし、 nConnect 対応クライアントでは、 1 つの NFS マウントに複数の TCP 接続（最大 16 個）を関連付けることができます。このような NFS クライアントは、ファイル操作を複数の TCP 接続にラウンドロビン方式で多重化し、使用可能なネットワーク帯域幅からより高いスループットを取得します。nConnect は、 NFSv3 マウントと NFSv4.1 マウントでのみ推奨されます。

NFS クライアントのマニュアルを参照して、 nConnect がクライアントバージョンでサポートされているかどうかを確認してください。

ONTAP 9.9.1 以降では、 NFSv4.1 がデフォルトで有効になっています。以前のリリースでは、を指定して有効にすることができました `-v4.1` オプションを選択し、に設定します `enabled` Storage Virtual Machine（SVM）にNFSサーバを作成する場合。

ONTAP は、 NFSv4.1 のディレクトリレベルおよびファイルレベルの委譲をサポートしていません。

NFSv4 4.2 の ONTAP サポート

ONTAP 9.8以降では、ONTAPでNFSv4.2プロトコルがサポートされ、NFSv4.2対応クライアントのアクセスが許可されます。

ONTAP 9.9.1 以降では、 NFSv4 4.2 がデフォルトで有効になっています。ONTAP 9.8では、 `-v4.1` オプションを選択し、に設定します `enabled` Storage Virtual Machine（SVM）にNFSサーバを作成する場合。NFSv4.1 を有効にすると、クライアントが v4.2 としてマウントされた状態で NFSv4.1 の機能を使用することもできます。

ONTAPの以降のリリースでは、NFSv4.2のオプション機能のサポートが拡張されています。

先頭のドキュメント	**NFSv4.2**のオプションの機能
ONTAP 9.12.1	• NFS拡張属性 • スパースファイル • スペースリザベーション
ONTAP 9.9.1	NFSとラベルされたMAC（必須アクセス制御

NFS v4.2セキュリティラベル

ONTAP 9.9.1以降では、NFSセキュリティラベルを有効にできます。デフォルトでは無効になっています。

NFS v4.2 セキュリティラベルでは、 ONTAP NFS サーバは必須アクセス制御（ MAC ）対応であり、クライアントから送信された sec_label 属性を保存および取得します。

詳細については、を参照してください "RFC 7240"。

ONTAP 9.12.1以降では、NDMPダンプ処理でNFS v4.2セキュリティラベルがサポートされます。以前のリリースのファイルまたはディレクトリでセキュリティラベルが検出された場合、ダンプは失敗します。

手順

1. 権限の設定を advanced に変更します。

```
set -privilege advanced
```

2. セキュリティラベルを有効にする：

```
vserver nfs modify -vserver _svm_name_ -v4.2-seclabel enabled
```

NFS拡張属性

ONTAP 9.12.1以降では、NFS拡張属性（xattrs）がデフォルトで有効になっています。

拡張属性は、で定義される標準のNFS属性です "RFC 8276" 最新のNFSクライアントで有効になっています。ユーザ定義のメタデータをファイルシステムオブジェクトに添付するために使用でき、高度なセキュリティの導入に役立ちます。

現在のところ、NDMPダンプ処理では、NFS拡張属性はサポートされていません。ファイルまたはディレクトリで拡張属性が検出された場合'ダンプは続行されますが'これらのファイルまたはディレクトリの拡張属性はバックアップされません

拡張属性を無効にする必要がある場合は、を使用します `vserver nfs modify -v4.2-xattrs disabled` コマンドを実行します

Parallel NFS の ONTAP サポート

ONTAP は、 Parallel NFS （ pNFS ；パラレル NFS ）をサポートします。pNFS プロトコルは、クラスタの複数のノードに分散されたファイルセットのデータにクライアントが直接アクセスできるようにして、パフォーマンスを向上します。これにより、クライアントはボリュームへの最適なパスを見つけることができます。

ハードマウントの使用

マウントの問題をトラブルシューティングするときは、正しい種類のマウントを使用していることを確認する必要があります。NFS は、ソフトマウントとハードマウントの 2

つのマウントタイプをサポートしています。信頼性を確保するために、ハードマウントのみを使用してください。

特に NFS タイムアウトが頻繁に発生する可能性がある場合は、ソフトマウントは使用しないでください。タイムアウトによって競合状態が発生し、データが破損する可能性があります。

NFS と SMB のファイルとディレクトリの命名規則

NFSとSMBのファイルとディレクトリの命名規則について説明します

ファイルとディレクトリの命名規則は、 ONTAP クラスタおよびクライアントの言語設定に加え、ネットワーククライアントのオペレーティングシステムとファイル共有プロトコルによって異なります。

オペレーティングシステムとファイル共有のプロトコルによって、次の要素が決定します。

- ファイル名に使用できる文字
- ファイル名での大文字と小文字の区別

ONTAP では、 ONTAP のリリースに応じて、ファイル、ディレクトリ、 qtree の名前でマルチバイト文字がサポートされます。

ファイル名またはディレクトリ名に使用できる文字

異なるオペレーティングシステムのクライアントからファイルやディレクトリにアクセスする場合は、どちらのオペレーティングシステムでも有効な文字を使用します。

たとえば、 UNIX を使用してファイルやディレクトリを作成する場合は、ファイル名やディレクトリ名にコロン（ : ）を使用しないでください。コロンは、 MS-DOS ファイル名やディレクトリ名では使用できないためです。有効な文字の制限はオペレーティングシステムごとに異なります。使用できない文字の詳細については、クライアントのオペレーティングシステムのマニュアルを参照してください。

マルチプロトコル環境でのファイル名とディレクトリ名の大文字と小文字の区別

ファイル名とディレクトリ名では、NFSクライアントでは大文字と小文字が区別されますが、SMBクライアントでは大文字と小文字が区別されません。この違いがマルチプロトコル環境に及ぼす影響と、 SMB 共有の作成時にパスを指定するときや、共有内のデータにアクセスするときにどのような対処が必要になるかを理解しておく必要があります。

SMBクライアントがという名前のディレクトリを作成する場合 `testdir`SMBクライアントと`NFS`クライアントのどちらでも、ファイル名はと表示されます `testdir`。ただし、SMBユーザがあとでディレクトリ名を作成しようとした場合 `TESTDIR`を指定することはできません。SMBクライアントでは、その名前がすでに存在しているとみなされます。NFSユーザがあとでという名前のディレクトリを作成する場合 `TESTDIR`では、NFSクライアントとSMBクライアントで表示されるディレクトリ名は次のように異なります。

- NFSクライアントでは、両方のディレクトリ名が作成したとおりに表示されます（例：） `testdir` および `TESTDIR`ディレクトリ名では大文字と小文字が区別されるためです。

- SMB クライアントでは、 2 つのディレクトリを区別するために 8.3 形式の名前が使用されます。1 つのディレクトリにはベースファイル名が付けられます。追加のディレクトリには 8.3 形式のファイル名が割り当てられます。
  - SMBクライアントでは、が表示されます `testdir` および `TESTDI~1`。
  - ONTAP によってが作成されます `TESTDI~1` 2つのディレクトリを区別するディレクトリ名。

    この場合、 Storage Virtual Machine （ SVM ）での共有の作成時または変更時に共有パスを指定するときは、 8.3 形式の名前を使用する必要があります。

ファイルについても、SMBクライアントでが作成された場合と同様です `test.txt`SMBクライアントと`NFS`クライアントのどちらでも、ファイル名はと表示されます `text.txt`。ただし、SMBユーザがあとでを作成しようとした場合 `Test.txt`を指定することはできません。SMBクライアントでは、その名前がすでに存在しているとみなされます。NFSユーザがあとでという名前のファイルを作成した場合 `Test.txt`では、NFSクライアントとSMBクライアントで表示されるファイル名は次のように異なります。

- NFSクライアントでは、両方のファイル名が作成されたとおりに表示され、 `test.txt` および `Test.txt` ファイル名では大文字と小文字が区別されるためです。
- SMB クライアントでは、 2 つのファイルを区別するために 8.3 形式の名前が使用されます。1 つのファイルにはベースファイル名が付けられます。追加のファイルには 8.3 形式のファイル名が割り当てられます。
  - SMBクライアントでは、が表示されます `test.txt` および `TEST~1.TXT`。
  - ONTAP によってが作成されます `TEST~1.TXT` 2つのファイルを区別するためのファイル名。

> Vserver cifs character-mappingコマンドを使用して文字マッピングを作成した場合、通常は大文字と小文字が区別されないWindows検索では大文字と小文字が区別される可能性があります。これは、文字マッピングが作成されていて、ファイル名がその文字マッピングを使っている場合にのみ、ファイル名のルックアップで大文字小文字が区別されることを意味します。

ONTAP によるファイル名とディレクトリ名の作成方法

ONTAP は、 SMB クライアントからアクセスされるすべてのディレクトリ内にあるファイルまたはディレクトリに対して 2 つの名前が作成され、保持されます。元の長い名前と 8.3 形式の名前です。

名前が 8 文字を超える、または拡張子が 3 文字を超える（ファイルの場合）ファイル名やディレクトリ名について、 ONTAP は次のように 8.3 形式の名前を生成します。

- 名前が 6 文字を超える場合は、元のファイル名またはディレクトリ名が 6 文字に切り捨てられます。
- 切り捨て後に一意でなくなったファイル名またはディレクトリ名には、チルダ（ ~ ）と 1~5 の数字が追加されます。

  同様の名前が 6 つ以上存在するため数字が足りなくなった場合には、元の名前とは無関係な一意の名前が作成されます。

- ファイルの場合は、ファイル名の拡張子が 3 文字に切り捨てられます。

たとえば、NFSクライアントがという名前のファイルを作成するとします `specifications.html`ONTAP で作成される`8.3`形式のファイル名はです `specif~1.htm`。この名前がすでに存在する場合、 ONTAP は

ファイル名の最後に別の番号を使用します。たとえば、NFSクライアントがという名前の別のファイルを作成したとします `specifications_new.html`、8.3形式の `specifications_new.html` はです `specif~2.htm`。

マルチバイトを含むファイル名、ディレクトリ名、 **qtree** 名の **ONTAP** での処理

ONTAP 9.5 以降では、 4 バイトの UTF-8 エンコード形式の名前がサポートされるようになり、 Basic Multilingual Plane （ BMP ；基本多言語面）以外の Unicode 補助文字を含むファイル、ディレクトリ、ツリーの名前を作成および表示できるようになりました。以前のリリースでは、これらの補助文字はマルチプロトコル環境では正しく表示されませんでした。

4バイトのUTF-8エンコード名のサポートを有効にするには、でnew_utf8mb4_言語コードを使用できます `vserver` および `volume` コマンド・ファミリー。

- 次のいずれかの方法で新しいボリュームを作成する必要があります。
- ボリュームを設定しています `-language` 明示的なオプション：

  ```
  volume create -language utf8mb4 {…}
  ```

- ボリュームを継承しています `-language` オプションを指定して作成または変更したSVMから、次のオプションを選択します。

  ```
  vserver [create|modify] -language utf8mb4 {…}``volume create {…}
  ```

- ONTAP 9.6以前を使用している場合、utf8mb4をサポートするために既存のボリュームを変更することはできません。utf8mb4対応の新しいボリュームを作成し、クライアントベースのコピーツールを使用してデータを移行する必要があります。

  ONTAP 9.7P1以降を使用している場合は、utf8mb4の既存ボリュームをサポートリクエストで変更できます。詳細については、を参照してください "ONTAPでの作成後にボリュームの言語を変更できますか。"。

[+]
SVM は utf8mb4 をサポートするように更新できますが、既存のボリュームの言語コードは元の設定のままです。

[+]

> ⓘ 現在のところ、 4 バイトの UTF-8 文字を含む LUN 名はサポートされていません。

- 一般に、 Unicode 文字データは、 Windows ファイルシステムアプリケーションでは 16-bit Unicode Transformation Format （ UTF-16 ）、 NFS ファイルシステムでは 8-bit Unicode Transformation Format （ UTF-8 ）を使用して表現されます。

  ONTAP 9.5 よりも前のリリースでは、 Windows クライアントで作成された UTF-16 の補助文字を含む名前は、他の Windows クライアントには正しく表示されましたが、 NFS クライアントでは UTF-8 に正しく変換されませんでした。同様に、 NFS クライアントで作成された UTF-8 の補助文字を含む名前は、 Windows クライアントで UTF-16 に正しく変換されませんでした。

- ONTAP 9.4 以前を実行しているシステムで作成したファイル名に有効な追加文字が含まれている場合や無

効な追加文字が含まれている場合、 ONTAP はそれらのファイル名を拒否し、ファイル名が無効であることを示すエラーを返します。

この問題を回避するには、ファイル名に BMP 文字のみを使用して補助文字は使用しないようにするか、ONTAP 9.5 以降にアップグレードしてください。

Unicode 文字は qtree 名で使用できます。

- どちらかを使用できます `volume qtree` qtree名を設定または変更するには、コマンドファミリーまたはSystem Managerを使用します。
- 日本語や中国語などの Unicode 形式のマルチバイト文字を qtree 名に含めることができます。
- ONTAP 9.5 よりも前のリリースでは、 BMP 文字（つまり 3 バイトで表現可能な文字）のみがサポートされます。

> ONTAP 9.5 よりも前のリリースでは、 qtree の親ボリュームのジャンクションパスに、Unicode 文字を使用した qtree 名やディレクトリ名を含めることができます。。 `volume show` 親ボリュームの言語設定がUTF-8の場合は、コマンドでこれらの名前が正しく表示されます。ただし、親ボリュームの言語設定が UTF-8 のいずれかでない場合は、ジャンクションパスの一部が数値の NFS 名に置き換えられて表示されます。

- 9.5 以降のリリースでは、 qtree が utf8mb4 に対応したボリュームに含まれていれば、 qtree 名で 4 バイト文字がサポートされます。

ボリュームでの **SMB** ファイル名の変換のための文字マッピングを設定します

NFS クライアントは、 SMB クライアントと特定の Windows アプリケーションでは無効な文字を含むファイル名を作成できます。ボリュームにおけるファイル名の変換のための文字マッピングを設定できます。これにより、そのままでは無効な NFS 名を持つファイルに SMB クライアントからアクセスできます。

このタスクについて

SMB クライアントが NFS クライアントによって作成されたファイルにアクセスすると、 ONTAP はファイル名を調べます。ファイル名が有効な SMB ファイル名でない場合は（たとえば、コロンが含まれている場合）、 ONTAP は各ファイルに対して保持されている 8.3 形式のファイル名を返します。ただし、これにより、長いファイル名に重要な情報をエンコードするアプリケーションで問題が発生します。

したがって、異なるオペレーティングシステムを使用するクライアント間でファイルを共有する場合は、両方のオペレーティングシステムで有効な文字をファイル名に使用する必要があります。

ただし、 SMB クライアントで有効でない文字を含む NFS クライアントが作成したファイル名がある場合は、無効な NFS の文字を、 SMB と特定の Windows アプリケーションの両方で有効な Unicode 文字に変換するマッピングを定義できます。たとえば、この機能は CATIAR MCAD および Mathematica アプリケーションをサポートしていますが、同じ要件を持つほかのアプリケーションでも使用できます。

文字マッピングはボリューム単位で設定できます。

ボリュームで文字マッピングを設定する場合は、次の点に注意する必要があります。

- 文字マッピングは、ジャンクションポイントをまたいで適用されません。

文字マッピングは、各ジャンクションボリュームに対して明示的に設定する必要があります。

- 無効な文字を表す Unicode 文字が、通常はファイル名に使用されないようにする必要があります。これらの文字が使用されていた場合、不要なマッピングが発生します。

  たとえば ' コロン (:) をハイフン (-) にマップしようとした場合 ' ファイル名にハイフン (-) が正しく使用されていれば 'Windows クライアントが "a-b`" という名前のファイルにアクセスしようとすると ' その要求は NFS 名 "a:b`" にマップされます (望ましい結果ではありません)

- 文字マッピングを適用してもまだマッピングに無効な Windows 文字が含まれている場合、 ONTAP は Windows 8.3 ファイル名にフォールバックします。
- FPolicy 通知、 NAS 監査ログ、セキュリティトレースメッセージでは、マッピングされたファイル名が表示されます。
- タイプが DP である SnapMirror 関係が作成されても、ソースボリュームの文字マッピングはデスティネーション DP ボリュームにレプリケートされません。
- 大文字と小文字の区別：マッピングされた Windows 名は NFS 名に変換されるため、名前の検索は NFS のセマンティクスに従います。NFS ルックアップでは大文字と小文字が区別されるという事実も含まれます。つまり、マッピングされた共有にアクセスするアプリケーションは、 Windows の大文字と小文字を区別しない動作に依存しません。ただし、 8.3 形式の名前は大文字と小文字が区別されません。
- 部分マッピングまたは無効なマッピング：ディレクトリ列挙（「 dir 」）を実行しているクライアントに返すように名前をマッピングしたあと、結果の Unicode 名について Windows の有効性がチェックされます。その名前にまだ無効な文字が含まれている場合、または Windows で無効な文字が含まれている場合（「 . 」または空白で終わる場合など）は、無効な名前の代わりに 8.3 形式の名前が返されます。

ステップ

1. 文字マッピングを設定します。

   ```
   vserver cifs character-mapping create -vserver vserver_name -volume
   volume_name -mapping mapping_text, ...
   ```

   マッピングは、「 : 」で区切られたソース文字とターゲット文字のペアのリストで構成されます。文字は、 16 進数値で入力された Unicode 文字です。例： 3C ： E03C

   それぞれの最初の値 `mapping_text` コロンで区切られたペアは、変換するNFS文字の16進値です。2番目の値は、SMBで使用されるUnicode値です。マッピングのペアは一意である必要があります（ 1 対 1 のマッピングが存在する必要があります）。

   - ソースマッピング

     次の表に、ソースマッピングで許可されている Unicode 文字セットを示します。

Unicode 文字	印刷された文字	説明
0x01-0x19	該当なし	印刷されない制御文字
0x5C	\	バックスラッシュ
0x3a	：	コロン

0x2A	*	アスタリスク
0x3f	？	疑問符
0x22	"	引用符
0x3C	<	より小さい
0x3E	>	が次の値より大きい
0x7C		
縦線	0xb1	±

- ターゲットマッピング

  ターゲット文字には、 U+E0000…U+F8FF の範囲の Unicode の「私用領域」を指定できます。

例

次のコマンドは、 Storage Virtual Machine （ SVM ） vs1 上の「 data 」という名前のボリュームに文字マッピングを作成します。

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

SMB ファイル名の変換のための文字マッピングを管理するコマンド

FlexVol での SMB ファイル名の変換に使用する情報を作成、変更、表示したり、ファイル文字マッピングを削除したりすることで、文字マッピングを管理できます。

状況	使用するコマンド
新しいファイル文字マッピングを作成します	`vserver cifs character-mapping create`
ファイル文字マッピングに関する情報を表示する	`vserver cifs character-mapping show`

既存のファイル文字マッピングを変更します	`vserver cifs character-mapping modify`
ファイル文字マッピングを削除します	`vserver cifs character-mapping delete`

詳細については、各コマンドのマニュアルページを参照してください。